SUSE Linux Enterprise Desktop

11 SP4

www.suse.com

14 de julho de 2015

Guia de Administração

Guia de Administração

Sumário

Sobre este guia

Este guia é destinado a administradores profissionais de rede e sistema durante a operação do SUSE® Linux Enterprise. Sendo assim, ele se compromete exclusivamente em garantir que o SUSE Linux Enterprise seja configurado apropriadamente e que os serviços requisitados na rede estejam disponíveis para permitir que ele funcione perfeitamente logo após a instalação inicial. Este guia não abrange o processo que garante que o SUSE Linux Enterprise ofereça compatibilidade apropriada ao software aplicativo da sua empresa ou que sua funcionalidade principal atenda a tais requisitos. Ele assume que foi feita uma auditoria completa dos requisitos e que foi solicitada a instalação ou uma instalação de teste, visando tal auditoria.

Este guia contém o seguinte:

Suporte e tarefas comuns
: O SUSE Linux Enterprise oferece uma ampla variedade de ferramentas para personalizar diversos aspectos do sistema. Esta parte apresenta algumas delas.

Sistema
: Aprenda mais sobre o sistema operacional subjacente estudando esta parte. O SUSE Linux Enterprise suporta várias arquiteturas de hardware e, com isso, você pode adaptar seus próprios aplicativos para serem executados no SUSE Linux Enterprise. As informações do carregador de boot e do procedimento de boot ajudam você a compreender como o sistema Linux funciona e como os seus próprios aplicativos e scripts personalizados podem se fundir a ele.

Computadores móveis
: Os laptops, e a comunicação entre dispositivos móveis como PDAs ou telefones celulares, e o SUSE Linux Enterprise requerem atenção especial. Cuide da conservação da energia e da integração de diferentes dispositivos a um ambiente de rede que está sofrendo mudanças. Tenha contato também com tecnologias de segundo plano que fornecem a funcionalidade necessária.

Serviços
: O SUSE Linux Enterprise foi projetado para ser um sistema operacional de rede. O SUSE® Linux Enterprise Desktop inclui suporte de cliente para muitos serviços de rede. Ele se integra bem em ambientes heterogêneos, inclusive clientes e servidores MS Windows.

Solucionando problemas
: Apresenta uma visão geral de onde encontrar ajuda e documentação adicional caso você precise de mais informações ou queira realizar tarefas específicas no sistema. Encontre também uma compilação dos problemas e erros mais frequentes e saiba como resolvê-los sozinho.

Muitos capítulos neste manual contêm links para recursos adicionais de documentação. Isso inclui documentação adicional disponível no sistema assim como documentação disponível na Internet.

Para obter uma visão geral da documentação disponível para o seu produto e das atualizações de documentação mais recentes, consulte `http://www.suse.com/doc`.

1 Documentação disponível

Fornecemos versões em HTML e PDF de nossos manuais em idiomas diferentes. Os seguintes manuais deste produto estão disponíveis para usuários e administradores:

KDE User Guide (↑*KDE User Guide*)
: Apresenta a área de trabalho do KDE do SUSE Linux Enterprise Desktop. Fornece orientações a você durante o uso e a configuração da área de trabalho, além de ajudá-lo a executar tarefas principais. Ele se destina principalmente a usuários que desejam usar de forma eficiente a área de trabalho do KDE como a área de trabalho padrão.

Guia do Usuário do GNOME (↑*Guia do Usuário do GNOME*)
: Apresenta a área de trabalho do GNOME do SUSE Linux Enterprise Desktop. Fornece orientações a você durante o uso e a configuração da área de trabalho, além de ajudá-lo a executar tarefas principais. Este manual é destinado principalmente a usuários finais que desejam usar de forma eficiente a área de trabalho do GNOME como sua área de trabalho padrão.

Guia de Aplicativos (↑*Guia de Aplicativos*)
: Aprenda a usar e configurar os principais aplicativos de área de trabalho no SUSE Linux Enterprise Desktop. Este manual apresenta os browsers e os clientes de e-mail, bem como aplicativos de escritório e ferramentas de colaboração. Também aborda aplicativos gráficos e de multimídia.

Deployment Guide (↑*Deployment Guide*)
: Mostra como instalar sistemas únicos ou múltiplos e como explorar os recursos inerentes ao produto para uma infraestrutura de desenvolvimento. Escolha uma das diversas abordagens, que variam desde um servidor de instalação local ou em rede até uma implantação em massa usando uma técnica de instalação remota controlada, automatizada e altamente personalizada.

Guia de Administração (p i)
: Descreve as tarefas de administração do sistema, como manutenção, monitoramento e personalização de um sistema instalado inicialmente.

Security Guide (↑*Security Guide*)
: Introduz conceitos básicos de segurança do sistema, incluindo aspectos de segurança locais e de rede. Mostra como usar o software de segurança inerente ao produto, como o AppArmor (que permite especificar quais arquivos cada programa pode ler, gravar e executar), e o sistema de auditoria que coleta, de maneira confiável, as informações sobre eventos relacionados à segurança.

System Analysis and Tuning Guide (↑*System Analysis and Tuning Guide*)
: Um guia do administrador para detecção de problema, resolução e otimização. Saiba como inspecionar e otimizar seu sistema através de ferramentas de monitoramento e como gerenciar recursos com eficiência. Inclui também uma visão geral dos problemas comuns e das soluções, além dos recursos adicionais de ajuda e documentação.

Virtualization with Xen (↑*Virtualization with Xen*)
: Oferece uma introdução à tecnologia de virtualização de seu produto. Ele apresenta uma visão geral sobre os diversos campos dos tipos de aplicativo e de instalação de cada uma das plataformas suportadas pelo SUSE Linux Enterprise Server, assim como uma breve descrição do procedimento de instalação.

Além dos manuais abrangentes, vários guias de inicialização rápida estão disponíveis:

KDE Quick Start (↑*KDE Quick Start*)
: Apresenta uma rápida introdução da área de trabalho do KDE e de alguns dos principais aplicativos executados nela.

GNOME Quick Start (↑*GNOME Quick Start*)
: Apresenta uma rápida introdução da área de trabalho do GNOME e de alguns dos principais aplicativos executados nela.

LibreOffice.org Quick Start (↑*LibreOffice.org Quick Start*)
Apresenta uma rápida introdução à suíte do LibreOffice e seus módulos para escrever textos, trabalhar com planilhas ou criar gráficos e apresentações.

Inicialização Rápida da Instalação (↑*Inicialização Rápida da Instalação*)
Lista os requisitos do sistema e o orienta passo a passo durante a instalação do SUSE Linux Enterprise Desktop de um DVD ou de uma imagem ISO.

Inicialização Rápida de Auditoria do Linux
Fornece uma breve visão geral de como habilitar e configurar o sistema de auditoria e como executar tarefas principais, como configurar regras de auditoria, gerar relatórios e analisar os arquivos de registro.

Inicialização Rápida do AppArmor
Ajuda você a entender os principais conceitos do AppArmor®.

Encontre as versões HTML de grande parte dos manuais dos produtos no sistema instalado em `/usr/share/doc/manual` ou nos centros de Ajuda do seu desktop. Obtenha as atualizações mais atuais da documentação em `http://www.suse.com/doc` de onde você poderá fazer download das versões HTML ou PDF dos manuais referentes ao seu produto.

2 Comentários

Vários canais de comentário estão disponíveis:

Solicitações de bugs e aperfeiçoamentos
Para ver as opções de serviços e suporte disponíveis ao seu produto, consulte `http://www.suse.com/support/`.

Para relatar bugs no componente de um produto, efetue login no Novell Customer Center em `http://www.suse.com/support/` e selecione *My Support (Meu Suporte)* > *Service Request (Solicitação de Serviço)*.

Comentários do usuário
Nós queremos saber a sua opinião e receber sugestões sobre este manual e outras documentações incluídas neste produto. Utilize o recurso Comentários na parte inferior de cada página da documentação online ou vá para `http://www.suse.com/doc/feedback.html` e digite lá os seus comentários.

E-mail
: Para fazer comentários sobre a documentação deste produto, você também pode enviar um e-mail para `doc-team@suse.de`. Inclua o título do documento, a versão do produto e a data de publicação da documentação. Para relatar erros ou fazer sugestões de melhorias, descreva resumidamente o problema e informe o respectivo número de seção e página (ou URL).

3 Convenções da documentação

As seguintes convenções tipográficas são usadas neste manual:

- `/etc/passwd`: nomes de diretório e nomes de arquivo
- *`marcador`*: substitua *`marcador`* pelo valor real
- `PATH`: a variável de ambiente PATH
- `ls`, `--help`: comandos, opções e parâmetros
- `user`: usuários ou grupos
- Alt, Alt + F1: uma tecla ou uma combinação de teclas a serem pressionadas; as teclas são mostradas em letras maiúsculas como aparecem no teclado
- *Arquivo*, *Arquivo* > *Gravar Como*: itens de menu, botões
- *Pinguins Dançarinos* (Capítulo *Pinguins*, ↑Outro Manual): É uma referência a um capítulo de outro manual.

Parte I. Suporte e tarefas comuns

1 Atualização Online do YaST

A Novell oferece um fluxo contínuo de atualizações de segurança de software para o seu produto. Por padrão, o applet de atualização é usado para manter o sistema atualizado. Consulte a Section “Keeping the System Up-to-date” (Chapter 6, *Installing or Removing Software*, ↑*Deployment Guide*) para obter mais informações sobre o applet de atualização. Este capítulo aborda a ferramenta alternativa para atualizar pacotes de software: Atualização Online do YaST.

Os patches atuais para o SUSE® Linux Enterprise Desktop estão disponíveis em um repositório de software de atualização. Se você registrou seu produto durante a instalação, já há um repositório de atualização configurado. Se você não registrou o SUSE Linux Enterprise Desktop, poderá fazer isso em *Software* > *Configuração de Atualização Online* no YaST e iniciar *Avançado* > *Registrar-se para obter suporte e repositório de atualizações*. Alternativamente, você pode adicionar manualmente um repositório de atualização de uma fonte confiável. Para adicionar ou remover repositórios, inicie o Gerenciador de Repositórios em *Software* > *Repositórios de Software* no YaST. Saiba mais sobre o Gerenciador de Repositórios na Section “Managing Software Repositories and Services” (Chapter 6, *Installing or Removing Software*, ↑*Deployment Guide*).

NOTA: erro ao acessar o catálogo de atualização

Se você não conseguir acessar o catálogo de atualização, pode ser que a assinatura tenha expirado. Normalmente, o SUSE Linux Enterprise Desktop vem com uma inscrição de um ou três anos, período em que você terá acesso ao catálogo de atualização. Esse acesso será negado quando a assinatura terminar.

No caso de uma negação de acesso ao catálogo de atualização, você verá uma mensagem de aviso com uma recomendação para visitar o Novell Customer Center e verificar sua assinatura. O Novell Customer Center está disponível em http://www.novell.com/center/.

Inclui atualizações com diferentes níveis de relevância:

Atualizações de Segurança
: Corrigem riscos à segurança e definitivamente devem ser instaladas.

Atualizações Recomendadas
: Corrigem problemas que podem comprometer o computador.

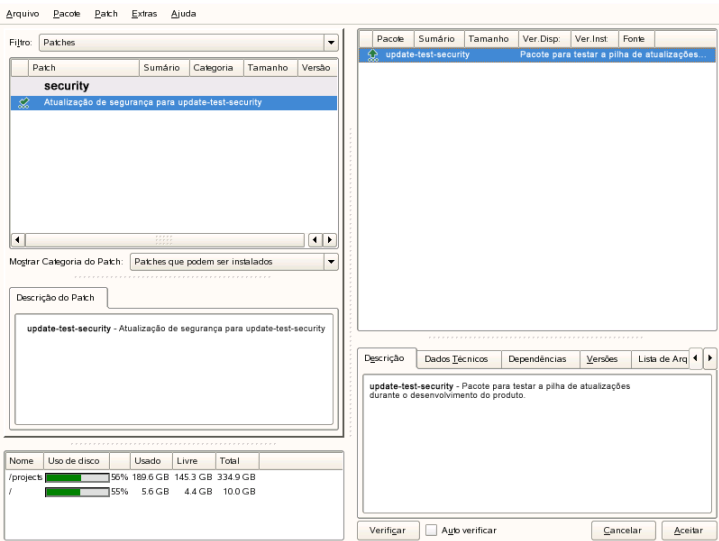
Atualizações Opcionais
: Corrigem problemas não relacionados à segurança ou aplicam melhorias.

1.1 Caixa de diálogo Atualização Online

A caixa de diálogo *Atualização Online* do YaST está disponível em dois tipos de kit de ferramentas: GTK (para GNOME) e Qt (para KDE). Ambas interfaces são diferentes na aparência, mas oferecem basicamente as mesmas funções. As seções a seguir apresentam uma breve descrição de cada. Para abrir a caixa de diálogo, inicie o YaST e selecione *Software* > *Atualização Online*. Se preferir, inicie-o usando a linha de comando `yast2 online_update`.

1.1.1 Interface do KDE (Qt)

A janela *Atualização Online* é composta por quatro seções.

Figura 1.1 Atualização Online do YaST: interface do Qt

A seção *Resumo* à esquerda lista os patches disponíveis para o SUSE Linux Enterprise Desktop. Os patches são classificados por relevância de segurança: `segurança`, `recomendado` e `opcional`. É possível mudar a tela da seção *Resumo* selecionando uma das seguintes opções em *Mostrar Categoria do Patch*:

Patches Necessários (tela padrão)
: Patches não instalados que se aplicam aos pacotes instalados no seu sistema.

Patches Não Necessários
: Os patches que se aplicam a pacotes não instalados no seu sistema, ou patches com requisitos que já foram atendidos (porque os pacotes relevantes já foram atualizados de outra fonte).

Todos os Patches
: Todos os patches disponíveis para o SUSE Linux Enterprise Desktop.

Cada entrada da lista na seção *Resumo* consiste em um símbolo e no nome do patch. Para obter uma visão geral dos símbolos possíveis e seu significado, pressione Shift + F1. As ações exigidas pelos patches de `Segurança` e `Recomendados` são predefinidas automaticamente. Essas ações são *Instalar automaticamente*, *Atualizar automaticamente* e *Apagar automaticamente*.

Se você instalar um pacote atualizado de um repositório que não seja o repositório de atualização, os requisitos de um patch para esse pacote poderão ser atendidos com essa instalação. Nesse caso, uma marca de seleção é exibida na frente do resumo do patch. O patch ficará visível na lista até você marcá-lo para instalação. Isso na verdade não instalará o patch (porque o pacote já está atualizado), mas marcará o patch como instalado.

Selecione uma entrada na seção *Resumo* para ver uma breve *Descrição do Patch* no canto inferior esquerdo da caixa de diálogo. A seção superior direita lista os pacotes incluídos no patch selecionado (um patch pode incluir vários pacotes). Clique em uma entrada na seção superior direita para ver os detalhes sobre o respectivo pacote que faz parte do patch.

1.1.2 Interface do GNOME (GTK)

A janela *Atualização Online* consiste em quatro seções principais.

Figura 1.2 Atualização Online do YaST: interface do GTK

A seção superior direita lista os patches disponíveis (ou já instalados) para o SUSE Linux Enterprise Desktop. Para filtrar os patches de acordo com sua relevância de segurança, clique na entrada *Prioridade* correspondente na seção superior esquerda da janela: `Segurança`, `Recomendado`, `Opcional` ou `Todos os patches`.

Se todos os patches disponíveis já estiverem instalados, a *Listagem de pacotes* na seção superior direita não mostrará nenhuma entrada. A caixa na seção inferior esquerda mostra o número dos patches disponíveis e já instalados e permite alternar a tela para ver os patches *Disponíveis* ou *Instalados*.

Selecione uma entrada na seção *Listagem de pacotes* para ver a descrição de um patch e mais detalhes no canto inferior direito na caixa de diálogo. Como o patch pode incluir vários pacotes, clique na entrada *Aplica-se a* na seção inferior direita para ver quais pacotes estão incluídos no respectivo patch.

Clique em uma entrada de patch para abrir uma linha com informações detalhadas sobre o patch na área inferior da janela. Aqui você pode ver uma descrição detalhada de um patch, bem como as versões disponíveis. Você também pode escolher *Instalar* patches opcionais; os patches de segurança e os recomendados já estão pré-selecionados para instalação.

1.2 Instalando patches

A caixa de diálogo Atualização Online do YaST permite instalar todos os patches disponíveis de uma vez ou selecionar manualmente os patches que deseja aplicar ao sistema. É possível também reverter os patches que foram aplicados ao sistema.

Por padrão, todos os novos patches (exceto os `opcionais`) disponíveis para o sistema já estão marcados para instalação. Eles serão aplicados automaticamente depois que você clicar em *Aceitar* ou *Aplicar*.

Procedimento 1.1 *Aplicando patches com a Atualização Online do YaST*

1 Inicie o YaST e selecione *Software* > *Atualização Online*.

2 Para aplicar automaticamente todos os novos patches (exceto os `opcionais`) disponíveis para o sistema, clique em *Aplicar* ou *Aceitar* para iniciar a instalação dos patches pré-selecionados.

3 Para modificar primeiro a seleção dos patches que deseja aplicar:

3a Use os respectivos filtros e telas fornecidos pelas interfaces GTK e Qt. Para obter os detalhes, consulte a Seção 1.1.1, "Interface do KDE (Qt)" (p 4) e a Seção 1.1.2, "Interface do GNOME (GTK)" (p 6).

3b Selecione ou anule a seleção dos patches de acordo com as suas necessidades e com a sua vontade, ativando ou desativando a respectiva caixa de seleção (GNOME) ou clicando o botão direito do mouse no patch e escolhendo a respectiva ação no menu de contexto (KDE).

IMPORTANTE: Sempre aplicar as atualizações de segurança

Não anule a seleção de nenhum patch relacionado à `segurança` se não tiver um bom motivo para isso. Eles corrigem riscos graves à segurança e impedem que o sistema seja explorado.

3c A maioria dos patches inclui atualizações para diversos pacotes. Para mudar as ações de pacotes únicos, clique o botão direito do mouse em um pacote na tela de pacotes e escolha uma ação (KDE).

3d Para confirmar sua seleção e aplicar os patches selecionados, clique em *Aplicar* ou *Aceitar*.

4 Após o término da instalação, clique em *Concluir* para sair da *Atualização Online* do YaST. Seu sistema está atualizado.

DICA: desabilitando deltarpms

Por padrão, o download das atualizações é feito como deltarpms. Como a reconstrução dos pacotes rpm dos deltarpms é uma tarefa que consome muita memória e capacidade do processador, certas instalações ou configurações de hardware podem exigir que você desabilite o uso de deltarpms em benefício do desempenho.

Para desabilitar o uso de deltarpms, edite o arquivo `/etc/zypp/zypp.conf` e defina `download.use_deltarpm` como `false`.

1.3 Atualização online automática

O YaST também permite configurar uma atualização automática com programação diária, semanal ou mensal. Para usar o respectivo módulo, você precisa instalar primeiro o pacote `yast2-online-update-configuration`.

Procedimento 1.2 *Configurando a atualização online automática*

1 Após a instalação, inicie o YaST e selecione *Software* > *Configuração de Atualização Online*.

Se preferir, inicie o módulo com `yast2 online_update_configuration` a partir da linha de comando.

2 Ative *Atualização Online Automática*.

3 Escolha se a atualização será *Diariamente*, *Semanalmente* ou *Mensalmente*.

   Alguns patches, como atualizações do kernel ou pacotes que exigem contratos de licença, requerem a interação do usuário, o que pode parar o procedimento de atualização automática.

4 Selecione se você deseja *Ignorar Patches Interativos* para que o procedimento de atualização continue até o fim automaticamente.

IMPORTANTE: Ignorando patches

Se você ignorar qualquer pacote que exija interação, execute a *Atualização Online* manual de tempos em tempos para instalar também esses patches. Do contrário, você poderá perder patches importantes.

---

5 Para aceitar automaticamente qualquer contrato de licença, ative *Agree with Licenses* (Concordar com Licenças).

6 Para instalar automaticamente todos os pacotes recomendados por pacotes atualizados, ative *Incluir Pacotes Recomendados*.

7 Para filtrar os patches por categoria (como segurança ou recomendado), ative *Filtrar por Categoria* e adicione as categorias de patch apropriadas da lista. Apenas os patches das categorias selecionadas serão instalados. Os outros serão ignorados.

8 Confirme sua configuração com *OK*.

2 Reunindo informações do sistema para suporte

Em caso de problemas, é possível criar um relatório detalhado do sistema com a ferramenta de linha de comando `supportconfig` ou o módulo de *Suporte* do YaST. Os dois coletam informações sobre o sistema, como a versão atual do kernel, o hardware, os pacotes instalados, a configuração da partição, etc. O resultado é um armazenamento de arquivos TAR. Após abrir uma Solicitação de Serviço (SS), você poderá fazer upload do armazenamento TAR para o Suporte Técnico Global. Ele ajuda a localizar o problema que você relatou e a orientá-lo para uma solução.

A ferramenta de linha de comando está incluída no pacote `supportutils`, que é instalado por padrão. O módulo de *Suporte* do YaST é baseado na ferramenta de linha de comando.

2.1 Coletando informações do sistema com o supportconfig

Para criar um armazenamento TAR com informações detalhadas do sistema que você possa enviar ao Suporte Técnico Global, use a ferramenta de linha de comando `supportconfig` diretamente ou o módulo de *Suporte* do YaST. A ferramenta de linha de comando está incluída no pacote `supportutils`, que é instalado por padrão. O módulo de *Suporte* do YaST também é baseado na ferramenta de linha de comando.

2.1.1 Criando um número de solicitação de serviço

É possível gerar armazenamentos do supportconfig a qualquer momento. No entanto, para enviar os dados do supportconfig ao Suporte Técnico Global, é necessário gerar primeiro um número de solicitação de serviço. Você precisa dele para fazer upload do armazenamento para o suporte.

Para criar uma solicitação de serviço, acesse `http://www.novell.com/center/eservice` e siga as instruções na tela. Anote o seu número de solicitação de serviço de 11 dígitos.

NOTA: Declaração de Privacidade

A SUSE e a Novell tratam os relatórios do sistema como dados confidenciais. Para ver detalhes do nosso compromisso de privacidade, acesse `http://www.novell.com/company/legal/privacy/`.

2.1.2 Destinos de upload

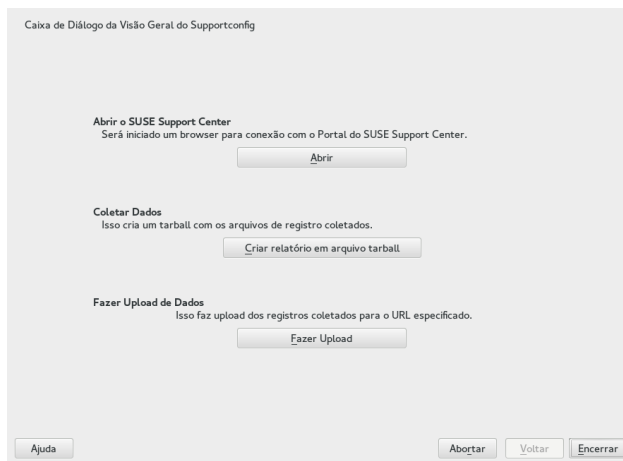
Após criar um número de solicitação de serviço, você poderá fazer upload dos armazenamentos supportconfig para o Suporte Técnico Global, conforme descrito no Procedimento 2.1, "Submetendo informações ao suporte com o YaST" (p 17) ou no Procedimento 2.2, "Submetendo informações ao suporte por linha de comando" (p 18). Use um dos seguintes destinos de upload:

- Clientes nos EUA: `ftp://ftp.novell.com/incoming`
- EMEA, Europa, Oriente Médio e África: `ftp://support-ftp.suse.com/in`

Você também pode anexar o armazenamento TAR manualmente à sua solicitação de serviço usando o URL da solicitação de serviço: `http://www.novell.com/center/eservice`.

2.1.3 Criando um armazenamento supportconfig com o YaST

Para usar o YaST para coletar informações do sistema, faça o seguinte:

1 Inicie o YaST e abra o módulo de *Suporte*.

2 Clique em *Criar relatório em arquivo tarball*.

3 Na janela seguinte, selecione uma das opções de supportconfig na lista de botões de opção. Por padrão, a opção *Usar Configurações (Técnicas) Personalizadas* está pré-selecionada. Para testar primeiro a função de relatório, use *Reunir apenas uma quantidade mínima de informações*. Para obter algumas informações básicas sobre outras opções, consulte a página de manual de `supportconfig`.

Continue com *Avançar*.

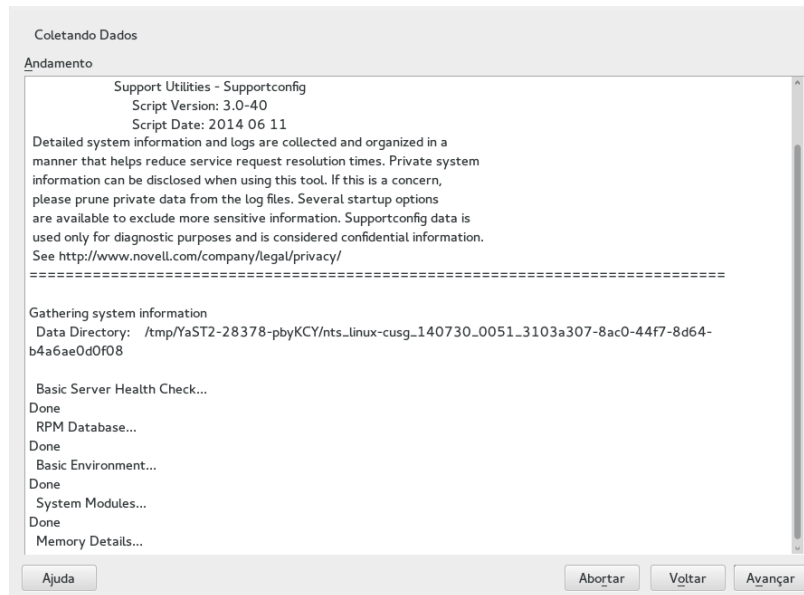
4 Digite suas informações de contato. Elas são gravadas em um arquivo chamado `basic-environment.txt` e incluídas no armazenamento que será criado.

5 Para submeter o armazenamento ao Suporte Técnico Global no fim do processo de coleta de informações, a opção *Informações de Upload* é obrigatória. O YaST propõe um servidor de upload automaticamente. Para modificá-lo, consulte a

Seção 2.1.2, “Destinos de upload” (p 12) para saber os detalhes de quais servidores de upload estão disponíveis.

Para submeter o armazenamento mais tarde, deixe a opção *Informações de Upload* vazia por enquanto.

6 Continue com *Avançar*.

7 A coleta de informações é iniciada.

Quando o processo for concluído, continue com *Avançar*.

8 Revise a coleta de dados: Selecione o *Nome do Arquivo* de um registro para ver seu conteúdo no YaST. Para remover arquivos do armazenamento TAR antes de submetê-lo ao suporte, use *Remover dos Dados*. Continue com *Avançar*.

9 Grave o armazenamento TAR. Se você iniciar o módulo do YaST como usuário `root`, por padrão, o YaST vai propor gravar o armazenamento em `/var/log` (ou em seu diretório pessoal). O formato do nome de arquivo é `nts_`*HOST_DATA_HORÁRIO*`.tbz`.

10 Para fazer upload do armazenamento diretamente para o suporte, verifique se a opção *Fazer upload do tarball com arquivos de registro para o URL* está ativada. O *Destino do Upload* mostrado aqui é aquele proposto pelo YaST no Passo 5 (p 13). Para modificar o destino do upload, encontre as informações detalhadas sobre quais servidores de upload estão disponíveis na Seção 2.1.2, “Destinos de upload” (p 12).

11 Para ignorar o upload, desative a opção *Fazer upload do tarball com arquivos de registro para o URL*.

12 Confirme as mudanças para fechar o módulo do YaST.

2.1.4 Criando um armazenamento supportconfig da linha de comando

O seguinte procedimento mostra como criar um armazenamento supportconfig, mas sem o submeter diretamente ao suporte. Para fazer seu upload, é necessário executar o comando com algumas opções, conforme descrito no Procedimento 2.2, “Submetendo informações ao suporte por linha de comando” (p 18).

1 Abra um shell e torne-se `root`.

2 Execute `supportconfig` sem nenhuma opção. Isso reúne as informações padrão do sistema.

3 Aguarde a ferramenta concluir a operação.

4 O local padrão do armazenamento é `/var/log`, com o formato de nome de arquivo `nts_`*`HOST_DATA_HORÁRIO`*`.tbz`

2.1.5 Opções comuns do supportconfig

O utilitário `supportconfig` é geralmente chamado sem nenhuma opção. Exiba uma lista de todas as opções com `supportconfig -h` ou consulte a página de manual. A seguinte lista apresenta uma breve visão geral de alguns casos de uso comuns:

Reduzindo o tamanho das informações coletadas
: Usar a opção mínima (`-m`):

```
supportconfig -m
```

Limitando as informações a determinado tópico
: Se você já localizou um problema com a saída padrão do `supportconfig` e descobriu que ele está relacionado apenas a determinada área ou conjunto de recursos, convém limitar as informações coletadas à área específica na próxima execução do `supportconfig`. Por exemplo, se você detectar problemas com o LVM e quiser testar uma recente mudança feita na configuração do LVM, convém coletar o mínimo de informações do supportconfig apenas sobre o LVM:

```
supportconfig -i LVM
```

Para ver a lista completa de palavras-chave de recursos que você pode usar para limitar as informações coletadas a determinada área, execute

```
supportconfig -F
```

Incluindo informações de contato adicionais na saída

```
supportconfig -E tux@example.org -N "Tux Penguin" -O "Penguin Inc." ...
```

(tudo em uma linha)

Coletando arquivos de registro já rotacionados

```
supportconfig -l
```

Isso é útil principalmente em ambientes de alto registro ou após uma falha do kernel quando o syslog gira os arquivos de registro após uma reinicialização.

2.2 Submetendo informações ao suporte técnico global

Use o módulo de *Suporte* do YaST ou o utilitário de linha de comando `supportconfig` para submeter as informações do sistema ao Suporte Técnico Global. Se você tiver um problema com o servidor e quiser a ajuda do suporte, precisará abrir primeiro uma solicitação de serviço. Para obter os detalhes, consulte a Seção 2.1.1, “Criando um número de solicitação de serviço” (p 12).

Os seguintes exemplos usam *12345678901* como marcador para o número da sua solicitação de serviço. Substitua *12345678901* pelo número da solicitação de serviço que você criou na Seção 2.1.1, "Criando um número de solicitação de serviço" (p 12).

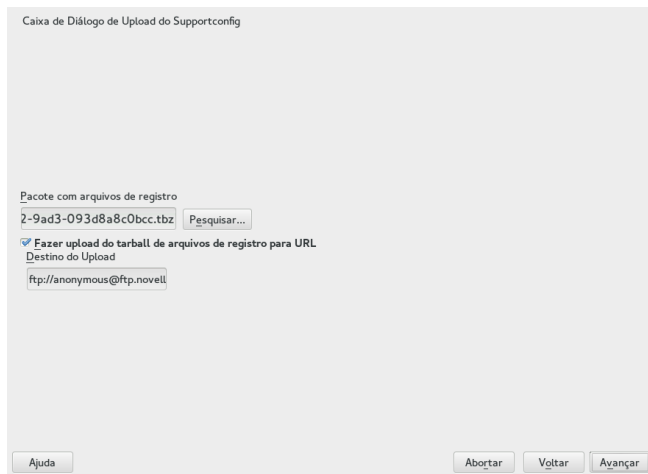
Procedimento 2.1 *Submetendo informações ao suporte com o YaST*

O seguinte procedimento considera que você já tenha criado um armazenamento supportconfig, mas ainda não tenha feito upload dele. Verifique se você incluiu suas informações de contato no armazenamento, conforme descrito na Seção 2.1.3, "Criando um armazenamento supportconfig com o YaST" (p 13), Passo 4. Para ver instruções de como gerar e submeter de uma só vez um armazenamento supportconfig, consulte a Seção 2.1.3, "Criando um armazenamento supportconfig com o YaST" (p 13).

1 Inicie o YaST e abra o módulo de *Suporte*.

2 Clique em *Fazer Upload*.

3 Em *Pacote com arquivos de registro*, especifique o caminho para o armazenamento supportconfig existente ou use *Pesquisar*.

4 O YaST propõe um servidor de upload automaticamente. Para modificá-lo, consulte a Seção 2.1.2, "Destinos de upload" (p 12) para saber os detalhes de quais servidores de upload estão disponíveis.

Continue com *Avançar*.

5 Clique em *Concluir*.

Procedimento 2.2 *Submetendo informações ao suporte por linha de comando*

O seguinte procedimento considera que você já tenha criado um armazenamento supportconfig, mas ainda não tenha feito upload dele. Para ver instruções de como gerar e submeter de uma só vez um armazenamento supportconfig, consulte a Seção 2.1.3, "Criando um armazenamento supportconfig com o YaST" (p 13).

1 Servidores com conectividade à Internet:

1a Para usar o destino de upload padrão, execute:

```
supportconfig -ur 12345678901
```

1b Para o destino de upload seguro, use o seguinte:

```
supportconfig -ar 12345678901
```

2 Servidores *sem* conectividade à Internet

2a Execute o seguinte:

```
supportconfig -r 12345678901
```

2b Faça upload do armazenamento `/var/log/nts_SR12345678901*tbz` manualmente para um de nossos servidores FTP. O servidor que deverá ser usado depende da sua localização global. Para uma visão geral, consulte a Seção 2.1.2, "Destinos de upload" (p 12).

3 Depois que o armazenamento TAR estiver no diretório de entrada do nosso servidor FTP, ele será automaticamente anexado à sua solicitação de serviço.

2.3 Suporte aos módulos do Kernel

Um requisito importante para todo sistema operacional empresarial é o nível de suporte que você recebe do ambiente. Os módulos do Kernel são o conector mais relevante entre o hardware ("controladoras") e o sistema operacional. Cada módulo do Kernel

no SUSE Linux Enterprise possui um flag `supported` (suportado) que pode ter três valores:

- “yes” (sim), portanto, `supported`
- “external” (externo), portanto, `supported`
- “” (vazio, não definido), portanto `unsupported` (não suportado)

As seguintes regras são válidas:

- Por padrão, todos os módulos de um Kernel autorrecompilado são marcados como não suportados.
- Os módulos do Kernel suportados pelos parceiros do SUSE e distribuídos pelo `SUSE SolidDriver Program` são marcados como “externos”.
- Se o flag `supported` não estiver definido, o carregamento do módulo contaminará o Kernel. Kernels contaminados não são suportados. Os módulos do Kernel não suportados são incluídos em um pacote RPM adicional (`kernel-`*`TIPO`*`-extra`) e não são carregados por padrão (*`TIPO`*=`default`|`xen`|...). Esses módulos não suportados também não estão disponíveis no instalador, e o pacote `kernel-`*`TIPO`*`-extra` não faz parte da mídia do SUSE Linux Enterprise.
- Os módulos do Kernel não incluídos em uma licença compatível com a licença do Kernel do Linux também contaminarão o Kernel. Para obter detalhes, consulte `/usr/src/linux/Documentation/sysctl/kernel.txt` e o estado de `/proc/sys/kernel/tainted`.

2.3.1 Informações técnicas

- Kernel do Linux: O valor de `/proc/sys/kernel/unsupported` usa o padrão `2` no SUSE Linux Enterprise 11 SP4 (`do not warn in syslog when loading unsupported modules`). Esse padrão é usado no instalador e no sistema instalado. Consulte `/usr/src/linux/Documentation/sysctl/kernel.txt` para obter mais informações.

- `modprobe`: O utilitário `modprobe` de verificação de dependências de módulos e carregamento dos módulos apropriados confirma se o valor do flag é `supported` (suportado). Se o valor for "sim" ou "externo", o módulo será carregado, do contrário, não. Para obter informações sobre como anular este comportamento, consulte a Seção 2.3.2, "Trabalhando com módulos não suportados" (p 20).

> **NOTA**
>
> Em geral, o SUSE não suporta a remoção de módulos de armazenamento por `modprobe -r`.

2.3.2 Trabalhando com módulos não suportados

Embora a capacidade de suporte geral seja importante, algumas situações podem exigir o carregamento de um módulo não suportado (por exemplo, para fins de teste ou depuração, ou se o fornecedor de hardware disponibilizar um hotfix).

- Para anular o padrão, edite `/etc/modprobe.d/unsupported-modules.conf` e mude o valor da variável `allow_unsupported_modules` para `1`. Se for necessário um módulo não suportado no initrd, lembre-se de executar `mkinitrd` para atualizar o initrd.

  Para apenas tentar carregar um módulo uma vez, é possível usar a opção `--allow-unsupported-modules` com `modprobe`. Para obter mais informações, consulte a página de manual de `modprobe`.

- Durante a instalação, módulos não suportados podem ser adicionados por meio de discos de atualização de driver, e eles serão carregados. Para impor o carregamento de módulos não suportados durante a inicialização e posteriormente, use a opção de linha de comando do Kernel `oem-modules`. Durante a instalação e inicialização do pacote `module-init-tools`, o flag do Kernel `TAINT_NO_SUPPORT` (`/proc/sys/kernel/tainted`) será avaliado. Se o Kernel já foi contaminado, `allow_unsupported_modules` será habilitado. Isso impede que módulos não suportados acessem o sistema que está sendo instalado. Se não houver nenhum módulo não suportado durante a instalação e não for usada a outra opção de linha de comando

especial do Kernel (oem-modules=1), o padrão ainda será de não permitir módulos não suportados.

Lembre-se de que carregar e executar módulos não suportados tornam o Kernel e todo o sistema não suportados pelo SUSE.

2.4 Para obter mais informações

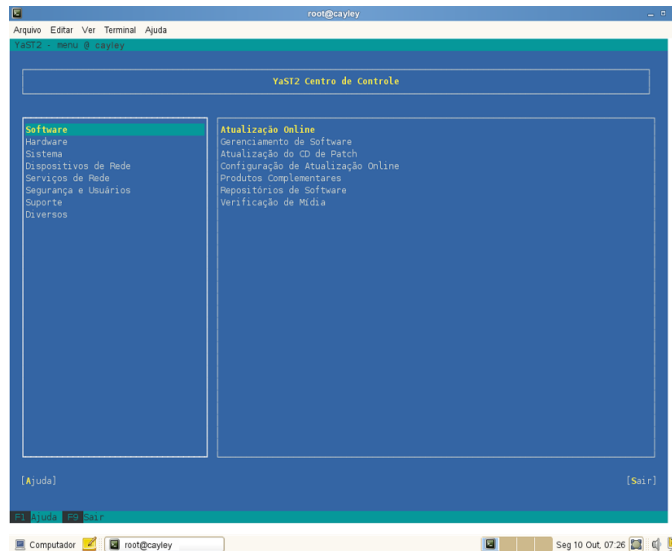
Obtenha mais informações sobre a coleta de informações do sistema nos seguintes documentos:

- man supportconfig: A página de manual de supportconfig.
- man supportconfig.conf: A página de manual do arquivo de configuração supportconfig.
- http://www.suse.com/communities/conversations/basic-server-health-check-supportconfig/: Uma verificação da saúde básica do servidor com o supportconfig.
- https://www.novell.com/communities/coolsolutions/cool_tools/create-your-own-supportconfig-plugin/: Criar seu próprio plug-in Supportconfig.
- http://www.suse.com/communities/conversations/creating-a-central-supportconfig-repository/: Criar um repositório central do Supportconfig.

3 YaST em modo de texto

Esta seção destina-se principalmente a administradores e especialistas do sistema que não executam um servidor X em seus sistemas e dependem da ferramenta de instalação baseada em texto. Ela contém informações básicas sobre como iniciar e operar o YaST em modo de texto.

O YaST em modo de texto usa a biblioteca ncurses para fornecer uma interface pseudográfica do usuário fácil. A biblioteca ncurses está instalada por padrão. O tamanho mínimo suportado do emulador de terminal no qual executar o YaST é de 80 x 25 caracteres.

Figura 3.1 *Janela principal do YaST em modo de texto*

Quando você inicia o YaST em modo de texto, o Centro de Controle do YaST é exibido (consulte a Figura 3.1). A janela principal contém três áreas: O quadro esquerdo apresenta as categorias às quais pertencem os vários módulos. Esse frame torna-se ativo quando o YaST é iniciado e, portanto, é marcado por uma borda branca em negrito. A categoria ativa é realçada. O quadro direito apresenta uma visão geral dos módulos disponíveis na categoria ativa. O frame inferior contém os botões *Ajuda* e *Sair*.

Quando você inicia o Centro de Controle do YaST, a categoria *Software* é selecionada automaticamente. Use ↓ e ↑ para mudar a categoria. Para selecionar um módulo da categoria, ative o frame direito com → e, em seguida, use ↓ e ↑ para selecionar o módulo. Mantenha as teclas de seta pressionadas para rolar pela lista de módulos disponíveis. O módulo selecionado fica realçado. Pressione Enter para iniciar o módulo ativo.

Vários botões ou campos de seleção no módulo contêm uma letra realçada (amarelo por padrão). Use Alt + letra_realçada para selecionar um botão diretamente, em vez de navegar até ele com Tab. Saia do Centro de Controle do YaST pressionando Alt + Q ou selecionando *Sair* e pressionando Enter.

DICA: Atualizando a janela de diálogo do YaST

Se uma janela de diálogo do YaST for corrompida ou distorcida (por exemplo, ao redimensionar a janela), pressione Ctrl + L para atualizar e restaurar seu conteúdo.

3.1 Navegação em módulos

A seguinte descrição dos elementos de controle nos módulos do YaST pressupõe que todas as teclas de função e combinações de teclas Alt funcionam e que não estão atribuídas a funções globais diferentes. Leia a Seção 3.2, "Restrição de combinações de tecla" (p 26) para obter informações sobre possíveis exceções.

Navegação entre botões e listas de seleção
: Use Tab para navegar entre os botões e frames contendo listas de seleção. Para navegar na ordem inversa, use Alt + Tab ou combinações de Shift + Tab.

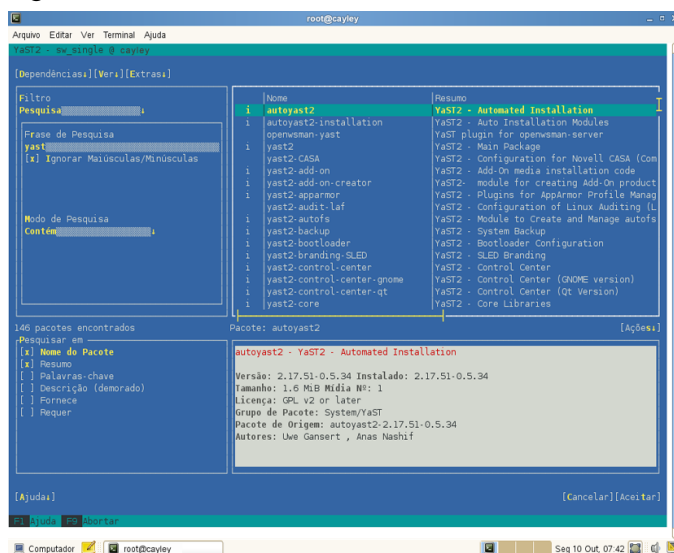
Navegação em listas de seleção
: Use as teclas de seta (↑ e ↓) para navegar entre os elementos individuais em um frame ativo que contenha uma lista de seleções. Se entradas individuais em um frame excederem a sua largura, use Shift + → ou Shift + ← para mover a barra de rolagem horizontalmente para a direita e esquerda. Alternativamente, use Ctrl + E ou Ctrl + A. Essa combinação também poderá ser utilizada se o uso de → ou ← resultar na mudança do frame ativo ou da lista de seleções atual, como no Centro de Controle.

Botões, botões de opção e caixas de seleção
: Para selecionar botões com colchetes vazios (caixas de seleção) ou parênteses vazios (botões de opção), pressione Espaço ou Enter. Alternativamente, pode-se selecionar botões de opção e caixas de seleção diretamente com Alt + letra_realçada. Nesse caso, não é necessário confirmar com Enter. Se você navegar até um item com Tab, pressione Enter para executar a ação selecionada ou ativar o item de menu respectivo.

Teclas de função
: As teclas F (F1 a F12) permitem acesso rápido aos vários botões. Os atalhos de teclas F disponíveis aparecem na linha inferior da tela do YaST. As teclas de função que são realmente mapeadas para cada botão dependem do módulo do YaST ativo,

pois módulos diferentes oferecem botões diferentes (Detalhes, Informações, Adicionar, Apagar, etc.). Use F10 para *Aceitar*, *OK*, *Avançar* e *Concluir*. Pressione F1 para acessar a ajuda do YaST.

Usando a árvore de navegação no modo ncurses
: Alguns módulos do YaST usam uma árvore de navegação na parte esquerda da janela para seleção de caixas de diálogo de configuração. Use as teclas de seta (↑ e ↓) para navegar na árvore. Use Espaço para abrir ou fechar itens de árvore. No modo ncurses, você deve pressionar Enter após uma seleção na árvore de navegação, a fim de mostrar a caixa de diálogo selecionada. Esse é um comportamento intencional que visa reduzir o tempo gasto para redesenhar durante a navegação na árvore.

Figura 3.2 *Módulo de instalação de software*

3.2 Restrição de combinações de tecla

Se o seu gerenciador de janelas usar combinações Alt globais, as combinações Alt no YaST talvez não funcionem. Teclas como Alt ou Shift também podem ser ocupadas pelas configurações do terminal.

Substituindo por AltEsc
: Os atalhos com Alt podem ser executados com Esc em vez de Alt. Por exemplo, Esc – H substitui Alt + H. (Primeiro pressione Esc, *depois* H.)

Navegação para trás e para frente com Ctrl + F e Ctrl + B
: Se as combinações de Alt e Shift estiverem ocupadas pelo gerenciador de janelas ou pelo terminal, use as combinações Ctrl + F (para frente) e Ctrl + B (para trás).

Restrição de teclas de função
: As teclas F também são usadas para funções. Certas teclas de função podem estar ocupadas pelo terminal e talvez não estejam disponíveis para o YaST. No entanto, as combinações de teclas Alt e teclas de função devem estar sempre disponíveis em um console de texto puro.

3.3 Opções de linha de comando do YaST

Além da interface de modo de texto, o YaST oferece uma interface de linha de comando pura. Para obter uma lista das opções de linha de comando do YaST, digite:

```
yast -h
```

3.3.1 Iniciando os módulos individuais

Para economizar tempo, os módulos do YaST individuais podem ser iniciados diretamente. Para iniciar um módulo, digite:

```
yast <module_name>
```

Exiba uma lista de todos os nomes de módulos disponíveis no seu sistema com `yast -l` ou `yast --list`. Inicie o módulo de rede, por exemplo, com `yast lan`.

3.3.2 Instalando pacotes a partir da linha de comando

Se você sabe o nome de um pacote e este é fornecido por qualquer um dos seus repositórios de instalação ativos, você pode usar a opção de linha de comando `-i` para instalar o pacote:

```
yast -i <package_name>
```

ou

```
yast --install <package_name>
```

`nome_do_pacote` pode ser um único nome curto de pacote, por exemplo `gvim`, instalado com verificação de dependência, ou o caminho completo para um pacote rpm, instalado sem verificação de dependência.

Se precisar de um utilitário de gerenciamento de software baseado em linha de comando com funcionalidade adicional à fornecida pelo YaST, considere usar o zypper. Esse novo utilitário usa a mesma biblioteca de gerenciamento de software que também é a base do gerenciador de pacote do YaST. O uso básico do Zypper está apresentado na Seção 7.1, "Usando o zypper" (p 69).

3.3.3 Parâmetros de linha de comando dos módulos do YaST

Para usar a funcionalidade do YaST em scripts, ele oferece suporte a linha de comando para módulos individuais. Nem todos os módulos têm suporte para linha de comando. Para exibir as opções disponíveis de um módulo, digite:

```
yast <module_name> help
```

Se um módulo não fornecer suporte para linha de comando, ele será iniciado no modo de texto e a seguinte mensagem aparecerá:

```
This YaST module does not support the command line interface.
```

Instantâneos/Rollback com o Snapper

4

Criar instantâneos do sistema de arquivos com a funcionalidade de fazer rollbacks no Linux era um recurso bastante solicitado no passado. O Snapper, em conjunto com o sistema de arquivos `Btrfs` ou os volumes LVM com aprovisionamento dinâmico, agora cumpre esse papel.

O `Btrfs`, um novo sistema de arquivos de gravação de cópia do Linux, suporta instantâneos de sistema de arquivos (uma cópia do estado de um subvolume em determinado ponto no tempo) de subvolumes (um ou mais sistemas de arquivos que podem ser montados separadamente em cada partição física). O Snapper permite gerenciar esses instantâneos. O Snapper vem com uma linha de comando e uma interface do YaST.

Por padrão, o Snapper e o `Btrfs` no SUSE Linux Enterprise Desktop são configurados para atuar como uma “ferramenta de desfazer” mudanças no sistema feitas com o YaST e o zypper. Antes e após a execução de um módulo do YaST ou do zypper, um instantâneo é criado. O Snapper permite comparar os dois instantâneos e dispõe de meios para reverter as diferenças entre ambos. As ferramentas também oferecem backups do sistema criando instantâneos a cada hora dos subvolumes do sistema.

4.1 Requisitos

Como o `Btrfs` é o único sistema de arquivos no SUSE Linux Enterprise Desktop que suporta instantâneos, ele é necessário em todas as partições ou subvolumes dos quais você deseja criar “instantâneos”.

4.1.1 Instantâneos e espaço em disco

Quando um instantâneo é criado, tanto o instantâneo quanto o original apontam para os mesmos blocos no sistema de arquivos. Por isso, o instantâneo inicialmente não ocupa espaço adicional no disco. Se os dados do sistema de arquivos original forem modificados, os blocos dos dados modificados serão copiados, enquanto os blocos dos dados antigos serão mantidos no instantâneo. Portanto, o instantâneo ocupa a mesma quantidade de espaço que os dados modificados. Ao longo do tempo, a quantidade de espaço alocada por um instantâneo cresce constantemente. Como consequência, a exclusão de arquivos do sistema de arquivos `Btrfs` que contém instantâneos pode *não* liberar espaço em disco!

NOTA: Local do instantâneo

Os instantâneos residem sempre na mesma partição ou subvolume do qual foi "criado o instantâneo". Não é possível armazenar os instantâneos em uma partição ou um subvolume diferente.

Como resultado, as partições com os instantâneos precisam ser maiores que as partições "normais". A quantidade exata depende bastante do número de instantâneos mantidos e da quantidade de modificações de dados. De acordo com a prática, convém usar o dobro do tamanho que seria usado normalmente.

DICA: Liberando espaço/utilização do disco

Para liberar espaço em uma partição do `Btrfs` com instantâneos, é preciso apagar instantâneos desnecessários, e não arquivos. Os instantâneos antigos ocupam mais espaço do que os novos.

Como o `df` não mostra a utilização do disco correta nos sistemas de arquivos `Btrfs`, você precisa usar o comando `btrfs filesystem df` *`PONTO_DE_MONTAGEM`*. A exibição da quantidade de espaço em disco alocada por um instantâneo não é suportada pelas ferramentas do `Btrfs`.

O upgrade de um service pack para outro resulta em instantâneos que ocupam muito espaço em disco nos subvolumes do sistema, porque muitos dados são modificados (atualizações de pacotes). É recomendada a exclusão manual desses instantâneos quando eles não são mais necessários.

O Snapper também pode ser usado para criar e gerenciar instantâneos em volumes LVM com aprovisionamento dinâmico formatados com ext3 ou XFS (consulte a Seção 4.6, “Usando o Snapper em volumes LVM com aprovisionamento dinâmico” (p 49)).

4.2 Usando o Snapper para desfazer mudanças no sistema

O Snapper no SUSE Linux Enterprise Desktop é pré-configurado para atuar como uma ferramenta capaz de desfazer as mudanças feitas pelo `zypper` e pelo YaST. Para esta finalidade, o Snapper é configurado para criar um par de instantâneos antes e depois de cada execução do `zypper` e do YaST. O Snapper permite também restaurar arquivos do sistema que foram acidentalmente apagados ou modificados. Backups são criados de hora em hora para essa finalidade.

Por padrão, os instantâneos automáticos, conforme descrito anteriormente, são configurados para a partição raiz e seus subvolumes. Para disponibilizar os instantâneos para outras partições, como `/home`, é possível criar configurações personalizadas.

4.2.1 Desfazendo mudanças do YaST e Zypper

Se você configurar a partição raiz com o `Btrfs` durante a instalação, o Snapper, pré-configurado para fazer rollbacks das mudanças do YaST ou do Zypper, será instalado automaticamente. Sempre que você iniciar um módulo do YaST ou uma transação do Zypper, serão criados dois instantâneos: um “pré-instantâneo”, que captura o estado do sistema de arquivos antes do início do módulo, e um “pós-instantâneo” após o término do módulo.

Usando o módulo Snapper do YaST ou a ferramenta de linha de comando `snapper`, é possível desfazer as mudanças feitas pelo YaST/zypper restaurando os arquivos do “pré-instantâneo”. Pela comparação dos dois instantâneos, as ferramentas permitem ver quais arquivos foram modificados. É possível também exibir as diferenças entre as duas versões de um arquivo (diff).

Como o Linux é um sistema multitarefa, processos diferentes do YaST ou do Zypper podem modificar os dados no período entre o pré e o pós-instantâneo. Se esse for o caso, a reversão completa para o pré-instantâneo vai desfazer também as mudanças realizadas por outros processos. Na maioria dos casos, isso seria indesejado; no entanto, é altamente recomendável para revisar detalhadamente as mudanças entre os dois instantâneos antes de iniciar o rollback. Se houver mudanças de outros processos para manter, selecione os arquivos para voltar.

IMPORTANTE: Limitações

Você deve conhecer as limitações do Snapper antes de tentar usar seu mecanismo de rollback. Consulte a Seção 4.4, “Limitações” (p 47) para obter os detalhes.

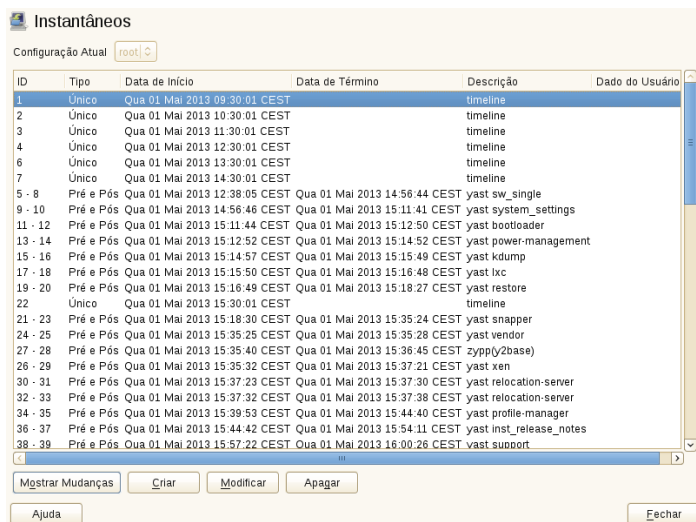
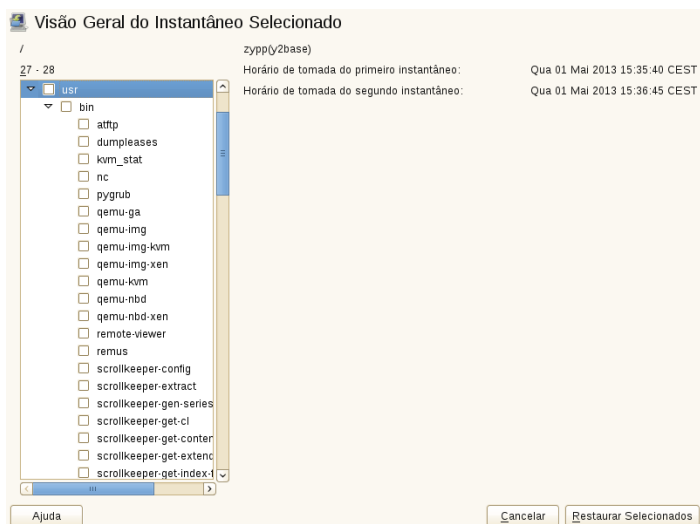
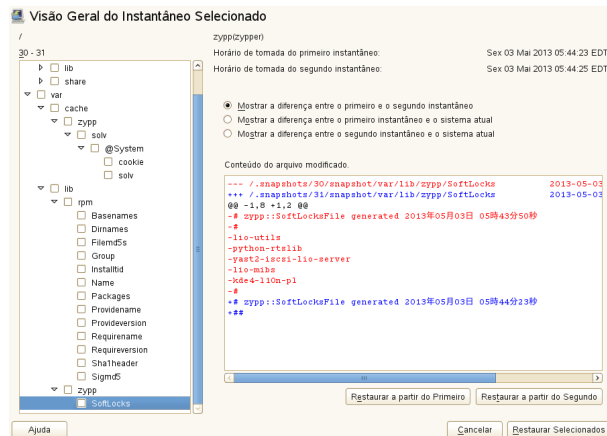
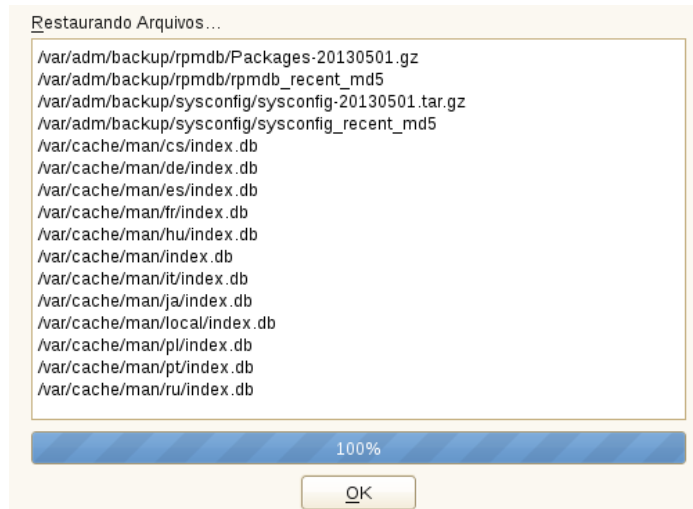
NOTA: Tempo de armazenamento de instantâneos

Por padrão, os últimos 100 instantâneos do YaST e do Zypper são mantidos. Se esse número for excedido, o(s) instantâneo(s) mais antigo(s) será(ão) apagado(s).

Procedimento 4.1 *Desfazendo mudanças usando o módulo Snapper do YaST*

1. Inicie o módulo *Snapper* pela seção *Diversos* no YaST ou digitando `yast2 snapper`.

2. Confirme se a *Configuração Atual* está definida como *root*. Esse é sempre o caso, a não ser que você tenha adicionado manualmente configurações personalizadas do Snapper.

3. Escolha o par de pré e pós-instantâneos na lista. Ambos os pares de instantâneos do YaST e do Zypper são do tipo *Pré e Pós*. Os instantâneos do YaST são denominados `yast` *`nome_do_módulo`* na *coluna Descrição*; os instantâneos do Zypper são denominados `zypp(zypper)`.

4 Clique em *Mostrar Mudanças* para abrir a lista de arquivos que são diferentes entre os dois instantâneos. A imagem a seguir mostra uma lista dos arquivos que foram modificados após adicionarem o `testador` do usuário.

5 Revise a lista de arquivos. Para exibir a diferença (“diff”) entre a versão pré e pós de um arquivo, selecione-o na lista. As imagens a seguir mostram as mudanças em `/etc/passwd` após a adição do `testador` do usuário.

6 Para restaurar um conjunto de arquivos, selecione os arquivos ou diretórios relevantes marcando a respectiva caixa de seleção. Clique em *Restaurar Selecionados* e clique em *Sim* para confirmar a ação.

Para restaurar um único arquivo, ative sua tela de diff clicando em seu nome. Clique em *Restaurar a partir do Primeiro* e clique em *Sim* para confirmar sua seleção.

Procedimento 4.2 *Desfazendo mudanças usando o comando snapper*

1. Obtenha uma lista dos instantâneos do YaST e do Zypper executando o comando `snapper list -t pre-post`. Os instantâneos do YaST são denominados `yast` *`nome_do_módulo`* na *coluna Descrição*; os instantâneos do Zypper são denominados `zypp(zypper)`.

```
~ # snapper list -t pre-post
     Pre # | Post # | Pre Date                 | Post Date                | Description

------+--------+-------------------------+-------------------------+---------------------+

    4    | 5     | Tue Jan 10 14:39:14 2012 | Tue Jan 10 14:39:33 2012 | yast system_settings

     65    | 66     | Thu Jan 12 17:18:10 2012 | Thu Jan 12 17:18:23 2012 | zypp(zypper)
     68    | 69     | Thu Jan 12 17:25:46 2012 | Thu Jan 12 17:27:09 2012 | zypp(zypper)
    73    | 74    | Thu Jan 12 17:32:55 2012 | Thu Jan 12 17:33:13 2012 | yast system_settings

     75    | 76     | Thu Jan 12 17:33:56 2012 | Thu Jan 12 17:34:42 2012 | yast users
     77    | 92     | Thu Jan 12 17:38:36 2012 | Thu Jan 12 23:13:13 2012 | yast snapper
     83    | 84     | Thu Jan 12 22:10:33 2012 | Thu Jan 12 22:10:39 2012 | zypp(zypper)
     85    | 86     | Thu Jan 12 22:16:58 2012 | Thu Jan 12 22:17:09 2012 | zypp(zypper)
     88    | 89     | Thu Jan 12 23:10:42 2012 | Thu Jan 12 23:10:46 2012 | zypp(zypper)
     90    | 91     | Thu Jan 12 23:11:40 2012 | Thu Jan 12 23:11:42 2012 | zypp(zypper)
     108   | 109    | Fri Jan 13 13:01:06 2012 | Fri Jan 13 13:01:10 2012 | zypp(zypper)
```

2. Obtenha uma lista dos arquivos modificados de um par de instantâneos com `snapper status` *`PRÉ`*`..`*`PÓS`*. Os arquivos com mudanças de conteúdo são marcados com *c*, os arquivos que foram adicionados são marcados com + e os arquivos apagados são marcados com -. O exemplo a seguir mostra o par de instantâneos da instalação do pacote `ncftp`.

```
~ # snapper status 108..109
     +... /usr/bin/ncftp
     +... /usr/bin/ncftpbatch
     +... /usr/bin/ncftpget
     +... /usr/bin/ncftpls
     [...]
     +... /usr/share/man/man1/ncftpspooler.1.gz
     c... /var/cache/zypp/solv/@System/cookie
     c... /var/cache/zypp/solv/@System/solv
     c... /var/lib/rpm/Basenames
     c... /var/lib/rpm/Dirnames
     c... /var/lib/rpm/Filemd5s
     c... /var/lib/rpm/Group
     c... /var/lib/rpm/Installtid
```

```
    c... /var/lib/rpm/Name
    c... /var/lib/rpm/Packages
    c... /var/lib/rpm/Providename
    c... /var/lib/rpm/Provideversion
    c... /var/lib/rpm/Requirename
    c... /var/lib/rpm/Requireversion
    c... /var/lib/rpm/Sha1header
    c... /var/lib/rpm/Sigmd5
    c... /var/lib/zypp/SoftLocks
```

3 Para exibir a diff de determinado arquivo, execute `snapper diff` *`PRÉ`*`..`*`PÓS`* *`NOMEDOARQUIVO`*. Se você não especificar *`NOMEDOARQUIVO`*, será exibida a diff de todos os arquivos.

```
~ # snapper diff 108..109 /var/lib/zypp/SoftLocks
     --- /.snapshots/108/snapshot/var/lib/zypp/SoftLocks 2012-01-12
23:15:22.408009164 +0100
     +++ /.snapshots/109/snapshot/var/lib/zypp/SoftLocks 2012-01-13
13:01:08.724009131 +0100
     @@ -1,4 +1,2 @@
     -# zypp::SoftLocksFile generated Thu Jan 12 23:10:46 2012
     -#
     -ncftp
     -#
     +# zypp::SoftLocksFile generated Fri Jan 13 13:01:08 2012
     +##
```

4 Para restaurar um ou mais arquivos, execute `snapper -v undochange` *`PRÉ`*`..`*`PÓS`* *`NOMESDOSARQUIVOS`*. Se você não especificar os *`NOMESDOSARQUIVOS`*, todos os arquivos serão restaurados.

```
~ # snapper -v undochange 108..109
     create:0 modify:16 delete:21
     undoing change...
     deleting /usr/share/man/man1/ncftpspooler.1.gz
     deleting /usr/share/man/man1/ncftpput.1.gz
     [...]
     deleting /usr/bin/ncftpls
     deleting /usr/bin/ncftpget
     deleting /usr/bin/ncftpbatch
     deleting /usr/bin/ncftp
     modifying /var/cache/zypp/solv/@System/cookie
     modifying /var/cache/zypp/solv/@System/solv
     modifying /var/lib/rpm/Basenames
     modifying /var/lib/rpm/Dirnames
     modifying /var/lib/rpm/Filemd5s
     modifying /var/lib/rpm/Group
     modifying /var/lib/rpm/Installtid
     modifying /var/lib/rpm/Name
```

```
modifying /var/lib/rpm/Packages
modifying /var/lib/rpm/Providename
modifying /var/lib/rpm/Provideversion
modifying /var/lib/rpm/Requirename
modifying /var/lib/rpm/Requireversion
modifying /var/lib/rpm/Sha1header
modifying /var/lib/rpm/Sigmd5
modifying /var/lib/zypp/SoftLocks
undoing change done
```

4.2.2 Usando o Snapper para restaurar arquivos dos backups por hora

Além dos instantâneos do YaST e do Zypper, o Snapper cria instantâneos a cada hora da partição do sistema (`/`). É possível usar os instantâneos do backup para restaurar arquivos apagados ou modificados por engano sem meios de recuperação. Usando o recurso diff do Snapper, é possível também descobrir quais modificações foram feitas em determinado momento.

Os instantâneos do backup por hora são do tipo `Single` e estão marcados com a descrição `timeline`. Para restaurar os arquivos desses instantâneos conforme descrito em Procedimento 4.1, “Desfazendo mudanças usando o módulo *Snapper* do YaST” (p 32) ou Procedimento 4.2, “Desfazendo mudanças usando o comando `snapper`” (p 35).

NOTA: Tempo de armazenamento de instantâneos

Por padrão, o primeiro instantâneo dos últimos dez dias, meses e anos são mantidos. Para saber os detalhes, consulte Exemplo 4.1, “Exemplo de configuração de linha do tempo” (p 40).

4.2.3 Criando e modificando as configurações do Snapper

O comportamento do Snapper é definido em um arquivo de configuração específico de cada partição ou subvolume `Btrfs`. Esses arquivos de configuração residem em `/etc/snapper/configs/`. A configuração padrão instalada com o Snapper do diretório

/ é chamada `root`. Ela cria e gerencia os instantâneos do YaST e do Zypper, além do instantâneo de backup por hora do `/`.

É possível criar suas próprias configurações para outras partições formatadas com `Btrfs` ou subvolumes existentes em uma partição `Btrfs`. No exemplo a seguir, nós definimos uma configuração do Snapper para backup dos dados do servidor Web que residem em uma partição separada formatada por `Btrfs` montada em `/srv/www`.

É possível usar o próprio `snapper` ou o módulo *Snapper* do YaST para restaurar arquivos desses instantâneos. No YaST, você precisa selecionar a sua *Configuração Atual* ao especificar sua configuração para o `snapper` com o switch global `-c` (ex. `snapper -c myconfig list`).

Para criar uma nova configuração do Snapper, execute `snapper create-config`:

```
snapper -c www-data❶ create-config
   /srv/www❷
```

❶ Nome do arquivo de configuração.

❷ Ponto de montagem da partição ou do subvolume `Btrfs` para o instantâneo.

Esse comando cria um novo arquivo de configuração `/etc/snapper/config-templates/www-data` com valores padrão razoáveis (obtidos de `/etc/snapper/config-templates/default`).

DICA: Padrões de configuração

Os valores padrão de uma nova configuração são obtidos de `/etc/snapper/config-templates/default`. Para usar seu próprio conjunto de padrões, crie uma cópia desse arquivo no mesmo diretório e ajuste-o de acordo com as suas necessidades. Para usá-lo, especifique a opção `-t` com o comando create-config:

```
snapper -c www-data create-config -t my_defaults /srv/www
```

4.2.3.1 Ajustando o arquivo de configuração

Para ajustar o arquivo de configuração, modifique-o com um editor. Ele inclui os pares de chave/valor no formato de *`chave`*`=`*`valor`*. Só é possível mudar o *`valor`*.

SUBVOLUME
: Ponto de montagem da partição ou do subvolume para o instantâneo. Não alterar.

FSTYPE
: Tipo de sistema de arquivos da partição. Não alterar.

NUMBER_CLEANUP
: Define se é para apagar automaticamente os instantâneos antigos quando a quantidade total exceder o número especificado com NUMBER_LIMIT *e* a duração especificada com NUMBER_MIN_AGE. Valores válidos: yes, no

> **NOTA: Limite e duração**
>
> NUMBER_LIMIT e NUMBER_MIN_AGE são sempre avaliados juntos. Os instantâneos são apagados apenas quando ocorrem as *duas* condições. Para sempre manter determinado número de instantâneos independentemente de sua duração, defina NUMBER_MIN_AGE como 0. Por outro lado, para não manter os instantâneos após certa duração, defina NUMBER_LIMIT como 0.

NUMBER_LIMIT
: Define quantos instantâneos manter quando NUMBER_CLEANUP está definido como yes.

NUMBER_MIN_AGE
: Define a duração mínima em segundos do instantâneo antes de ser automaticamente apagado.

TIMELINE_CREATE
: Se definido como yes, serão criados instantâneos de hora em hora. Essa é a única forma de criar automaticamente os instantâneos, embora seja altamente recomendável defini-lo como yes. Valores válidos: yes, no

TIMELINE_CLEANUP
: Define se é para apagar automaticamente os instantâneos antigos quando a quantidade exceder o número especificado com as opções *TIMELINE_LIMIT_** *e* a duração especificada com TIMELINE_MIN_AGE. Valores válidos: yes, no

TIMELINE_MIN_AGE
: Define a duração mínima em segundos do instantâneo antes de ser automaticamente apagado.

TIMELINE_LIMIT_HOURLY, TIMELINE_LIMIT_DAILY, TIMELINE_LIMIT_MONTHLY, TIMELINE_LIMIT_YEARLY
: Número de instantâneos para manter por hora, dia, mês, ano.

Exemplo 4.1 *Exemplo de configuração de linha do tempo*

```
TIMELINE_CREATE="yes"
        TIMELINE_CLEANUP="yes"
        TIMELINE_MIN_AGE="1800"
        TIMELINE_LIMIT_HOURLY="10"
        TIMELINE_LIMIT_DAILY="10"
        TIMELINE_LIMIT_MONTHLY="10"
        TIMELINE_LIMIT_YEARLY="10"
```

Este exemplo de configuração habilita os instantâneos por hora, que são limpos automaticamente. TIMELINE_MIN_AGE e TIMELINE_LIMIT_* são sempre avaliados juntos. Neste exemplo, a duração mínima de um instantâneo, antes de ser apagado, está definida como 30 minutos (1800 segundos). Como nós criamos instantâneos por hora, isso garante que apenas os instantâneos mais recentes sejam mantidos. Se TIMELINE_LIMIT_DAILY não estiver definido como zero, significa que o primeiro instantâneo do dia também será mantido.

Instantâneos para manter

- De hora em hora: Os últimos dez instantâneos que foram criados.
- Diariamente: O primeiro instantâneo diário criado é mantido para os últimos dez dias.
- Mensalmente: O primeiro instantâneo criado no último dia do mês é mantido para os últimos dez meses.
- Anualmente: O primeiro instantâneo criado no último dia do ano é mantido para os últimos dez anos.

4.2.3.2 Usando o Snapper como usuário comum

Por padrão, o Snapper só pode ser usado pelo `root`. No entanto, há casos em que determinados grupos ou usuários precisam criar instantâneos ou desfazer mudanças revertendo um instantâneo:

- um administrador de site na Web deseja criar um instantâneo de `/srv/www`.
- um administrador de banco de dados deseja criar um instantâneo dos bancos de dados.
- um usuário deseja criar um instantâneo de seu diretório pessoal.

Para essas finalidades, é possível criar configurações do Snapper que concedam permissões a usuários ou grupos. Além da mudança nessa configuração, os usuários especificados devem conseguir ler e acessar o diretório `.snapshots` correspondente.

***Procedimento 4.3** Habilitando usuários comuns a usar o Snapper*

Observe que todas as etapas deste procedimento devem ser executadas pelo `root`.

1 Se não houver um, crie uma configuração do Snapper para a partição ou o subvolume em que o usuário consiga utilizar o Snapper. Consulte a Seção 4.2.3, “Criando e modificando as configurações do Snapper” (p 37) para obter instruções. Exemplo:

```
snapper --config web_data create /srv/www
```

2 O arquivo de configuração é criado em `/etc/snapper/configs/`*`NOME`*, em que NOME é o valor que você especificou com `-c/--config` na etapa anterior (por exemplo, `/etc/snapper/configs/web_data`). Ajuste-o de acordo com as suas necessidades. Consulte a Seção 4.2.3.1, “Ajustando o arquivo de configuração” (p 38) para obter os detalhes.

3 Defina os valores de `ALLOW_USERS` e `ALLOW_GROUPS` para conceder permissões a usuários e grupos, respectivamente. Separe várias entradas com Space. Para conceder permissões ao usuário `www_admin`; por exemplo, digite:

```
ALLOW_USERS="www_admin"
```

4 Conceda permissões de leitura e acesso ao diretório de instantâneos *`CAMINHO`*/.snapshots. *`CAMINHO`* deve ser substituído pelo subvolume especificado na primeira etapa deste procedimento. Exemplo:

```
chmod a+rx /srv/www/.snapshots
```

Agora o(s) usuário(s) e grupo(s) pode(m) utilizar a configuração especificada do Snapper. É possível testá-la com o comando `list`, por exemplo:

```
www_admin:~ > snapper -c web_data list
```

4.2.4 Desabilitando instantâneos automáticos

Se você configurou a partição raiz com `Btrfs` durante a instalação, o Snapper criará automaticamente instantâneos do sistema a cada hora, além de pré e pós-instantâneos das transações do YaST e do zypper. Cada uma dessas tarefas pode ser desabilitada da seguinte forma:

Desabilitando instantâneos por hora
: Edite `/etc/snapper/configs/root` e defina `TIMELINE_CREATE` como `no`:

```
TIMELINE_CREATE="no"
```

Desabilitando instantâneos do Zypper
: Desinstale o pacote `snapper-zypp-plugin`

Desabilitando instantâneos do YaST
: Edite `/etc/sysconfig/yast2` e defina `USE_SNAPPER` como `no`:

```
USE_SNAPPER="no"
```

4.3 Criando e gerenciando instantâneos manualmente

Não é possível apenas criar e gerenciar os instantâneos automaticamente pela configuração do Snapper, você também pode criar pares de instantâneos (“antes e após”) ou instantâneos únicos manualmente usando a ferramenta de linha de comando ou o módulo do YaST.

Todas as operações do Snapper são executadas de acordo com uma configuração existente (consulte a Seção 4.2.3, “Criando e modificando as configurações do Snapper” (p 37) para obter os detalhes). Você só pode criar instantâneo de partições ou volumes em que exista uma configuração. Por padrão, a configuração do sistema (`root`) é usada. Para criar ou gerenciar instantâneos com sua própria configuração, selecione-a de maneira clara. Use o menu suspenso *Configuração Atual* no YaST ou especifique `-c` na linha de comando (`snapper -c MINHACONFIG COMANDO`).

4.3.1 Metadados de instantâneos

Cada instantâneo consiste no próprio instantâneo e em alguns metadados. Ao criar um instantâneo, você também precisa especificar os metadados. A modificação de um instantâneo também altera seus metadados; não é possível modificar seu conteúdo. Os seguintes metadados estão disponíveis para cada instantâneo:

- **Tipo**: Tipo do instantâneo, consulte a Seção 4.3.1.1, “Tipos de instantâneos” (p 43) para obter os detalhes. Esses dados não podem ser mudados.

- **Número**: Número exclusivo do instantâneo. Esses dados não podem ser mudados.

- **Número do Pré**: Especifica o número do pré-instantâneo correspondente. Apenas para instantâneos do tipo pós. Esses dados não podem ser mudados.

- **Descrição**: A descrição do instantâneo.

- **Dados de usuário**: Uma descrição estendida que especifica os dados personalizados no formato de uma lista de chave=valor separada por vírgula: `reason=testing_stuff, user=tux`

- **Algoritmo de Limpeza**: Algoritmo de limpeza do instantâneo. Consulte a Seção 4.3.1.2, “Algoritmos de limpeza” (p 44) para obter os detalhes.

4.3.1.1 Tipos de instantâneos

O Snapper reconhece três tipos diferentes de instantâneos: pre (pré), post (pós) e single (único). Eles são iguais fisicamente, mas o Snapper trabalha com eles de forma diferente.

`pre`
: Instantâneo de um sistema de arquivos *antes* da modificação. Cada instantâneo `pre` tem o seu `post` correspondente. Por exemplo, usado para instantâneos automáticos do YaST/zypper.

`post`
: Instantâneo de um sistema de arquivos *após* a modificação. Cada instantâneo `post` tem o seu `pre` correspondente. Por exemplo, usado para instantâneos automáticos do YaST/zypper.

`single`
: Instantâneo independente. Usado, por exemplo, para instantâneos automáticos por hora. Esse é o tipo padrão quando se cria instantâneos.

4.3.1.2 Algoritmos de limpeza

O Snapper oferece três algoritmos para limpeza de instantâneos antigos. Os algoritmos são executados em uma tarefa cron diária. A frequência de limpeza é definida na configuração do Snapper para a partição ou o subvolume (consulte a Seção 4.2.3.1, “Ajustando o arquivo de configuração” (p 38) para obter os detalhes).

number
: Apaga instantâneos antigos quando determinado número de instantâneos é atingido.

time line
: Apaga instantâneos antigos que passaram de certa duração, mas mantém um número de instantâneos por hora, dia, mês e ano.

empty-pre-post
: Apaga os pares de pré/pós-instantâneos com diffs vazias.

4.3.2 Criando instantâneos

A criação do instantâneo é feita executando o comando `snapper create` ou clicando em *Criar* no módulo *Snapper* do YaST. Os exemplos a seguir explicam como criar instantâneos da linha de comando. Eles são fáceis de adotar ao usar a interface do YaST.

DICA: Descrição do instantâneo

Especifique sempre uma descrição significativa para no futuro conseguir identificar sua finalidade. É possível especificar ainda mais informações na opção de dados do usuário.

`snapper create --description "Snapshot for week 2 2013"`
: Cria um instantâneo independente (tipo único) na configuração padrão (`root`) com uma descrição. Como nenhum algoritmo de limpeza foi especificado, o instantâneo nunca será apagado automaticamente.

`snapper --config home create --description "Cleanup in ~tux"`
: Cria um instantâneo independente (tipo único) em uma configuração personalizada chamada `home` com uma descrição. Como nenhum algoritmo de limpeza foi especificado, o instantâneo nunca será apagado automaticamente.

`snapper --config home create --description "Daily data backup" --cleanup-algorithm timeline`
: Cria um instantâneo independente (tipo único) em uma configuração personalizada chamada `home` com uma descrição. O arquivo é apagado automaticamente quando atende aos critérios especificados no algoritmo de limpeza de linha do tempo da configuração.

`snapper create --type pre--print-number--description "Before the Apache config cleanup"`
: Cria um instantâneo do tipo `pre` e imprime o número do instantâneo. Primeiro comando necessário para criar um par de instantâneos usado para gravar o estado “antes” e “após”.

`snapper create --type post--pre-number 30--description "After the Apache config cleanup"`
: Cria um instantâneo do tipo `post` ligado a seu par `pre` de número `30`. Segundo comando necessário para criar um par de instantâneos usado para gravar o estado “antes” e “após”.

snapper create --command *COMANDO*--description "Before and after COMANDO"
: Cria automaticamente um par de instantâneos antes e após a execução do *COMANDO*. Essa opção só está disponível ao usar o snapper na linha de comando.

4.3.3 Modificando os metadados do instantâneo

O Snapper permite modificar a descrição, o algoritmo de limpeza e os dados de usuário de um instantâneo. Todos os outros metadados não podem ser mudados. Os exemplos a seguir explicam como modificar instantâneos da linha de comando. Eles são fáceis de adotar ao usar a interface do YaST.

Para modificar um instantâneo na linha de comando, você precisa saber o número dele. Use `snapper list` para exibir todos os instantâneos e seus números.

O módulo *Snapper* do YaST já lista todos os instantâneos. Escolha um na lista e clique em *Modificar*.

snapper modify --cleanup-algorithm "timeline" 10
: Modifica os metadados do instantâneo 10 na configuração padrão (`root`). O algoritmo de limpeza é definido como `timeline`.

snapper --config home modify --description "daily backup" -cleanup-algorithm "timeline"120
: Modifica os metadados do instantâneo 120 na configuração personalizada chamada `home`. Uma nova descrição é definida e o algoritmo de limpeza fica indefinido.

4.3.4 Apagando instantâneos

Para apagar um instantâneo com o módulo *Snapper* do YaST, escolha-o na lista e clique em *Apagar*.

Para apagar um instantâneo com a ferramenta de linha de comando, você precisa saber o número dele. Para saber, execute `snapper list`. Para apagar um instantâneo, execute `snapper delete` *NÚMERO*.

DICA: Apagando pares de instantâneos

Ao apagar um instantâneo `pre`, sempre apague seu `post` correspondente (e vice-versa).

`snapper delete 65`
: Apaga o instantâneo 65 na configuração padrão (`root`).

`snapper -c home delete 89 90`
: Apaga os instantâneos 89 e 90 na configuração personalizada chamada `home`.

DICA: Instantâneos antigos ocupam mais espaço em disco

Se você apagar instantâneos para liberar espaço no disco rígido (consulte a Seção 4.1.1, "Instantâneos e espaço em disco" (p 30) para obter os detalhes), apague primeiro os instantâneos antigos. Quanto mais antigo for o instantâneo, mais espaço em disco ele ocupa.

Os instantâneos também são automaticamente apagados por uma tarefa cron diária. Consulte a Seção 4.3.1.2, "Algoritmos de limpeza" (p 44) para obter os detalhes.

4.4 Limitações

Apesar de estarem prontos para produção, o `Btrfs` e o Snapper estão em constante desenvolvimento. As seguintes limitações existem no momento. Há planos de se resolver estes problemas em versões futuras.

4.4.1 Consistência de dados

Não existe um mecanismo que garanta a consistência dos dados na hora de criar um instantâneo. Sempre que um arquivo é gravado (ex. um banco de dados) ao mesmo tempo que um instantâneo é criado, o resultado é um arquivo danificado ou gravado parcialmente. A restauração desse arquivo causa problemas. Portanto, é altamente recomendável *sempre* revisar com cuidado a lista de arquivos modificados e suas diffs. Apenas restaure arquivos que realmente tenham que fazer parte da ação que deseja voltar.

4.4.2 Revertendo adições de usuário

Normalmente, /home reside em uma partição separada. Essa partição separada não faz parte da configuração padrão de rollbacks do YaST. Portanto, a partição pessoal do usuário não será apagada durante a reversão de uma adição de usuário com o Snapper. É altamente recomendável usar a ferramenta do YaST *Gerenciamento de Usuários e Grupos* para remover usuários.

4.4.3 Nenhuma mudança no rollback em /boot e no carregador de boot

O SUSE Linux Enterprise Desktop não pode ser inicializado de partições Btrfs. Portanto, uma partição separada para /boot é criada durante a instalação ao usar o Btrfs para a partição do sistema. Como /boot não suporta instantâneos, as seguintes restrições se aplicam aos rollbacks do YaST/zypper:

sem rollback de qualquer mudança de configuração no carregador de boot
: O único arquivo que pode ser voltado é o arquivo de configuração do carregador de boot em /etc. Os arquivos principais de configuração residem em /boot e não podem ser voltados.

sem rollback completo para instalações do Kernel
: O Kernel e seu initrd são instalados na partição /boot, enquanto os módulos ou as fontes do Kernel são instalados em /var/lib e /usr/src, respectivamente. Além disso, cada instalação do Kernel também muda os arquivos de configuração do carregador de boot em /boot. Portanto, sempre que fizer um rollback que envolva desfazer uma instalação do Kernel, você precisará remover manualmente o Kernel e seu initrd de /boot e ajustar a configuração do carregador de boot removendo a entrada de boot do Kernel.

4.5 Perguntas mais frequentes

Por que o Snapper nunca mostra as mudanças em `/var/log`, `/tmp` e em outros diretórios?

Para alguns diretórios, nós decidimos desabilitar a “criação de instantâneo”; por exemplo, `/var/log`, já que a reversão de registros dificulta a pesquisa por problemas. Para excluir um caminho de “criação de instantâneo”, nós criamos um subvolume para esse caminho. Os seguintes pontos de montagem não estão incluídos na “criação de instantâneo” no SUSE Linux Enterprise Desktop:

- `/opt`
- `/srv`
- `/tmp`
- `/var/crash`
- `/var/log`
- `/var/run`
- `/var/spool`
- `/var/tmp`

Posso inicializar um instantâneo do carregador de boot?

Isso não é possível no momento. O carregador de boot no SUSE Linux Enterprise Desktop não suporta inicialização de uma partição `Btrfs`.

4.6 Usando o Snapper em volumes LVM com aprovisionamento dinâmico

Além dos instantâneos em sistemas de arquivos `Btrfs`, o snapper também suporta a “criação de instantâneo” em volumes LVM com aprovisionamento dinâmico

(instantâneos em volumes LVM comuns *não* são suportados) formatados com ext3 ou XFS. Para obter mais informações e instruções de configuração, consulte a Section "LVM Configuration" (Chapter 12, *Advanced Disk Setup*, ↑*Deployment Guide*).

Para usar o Snapper em um volume LVM com aprovisionamento dinâmico, crie para ele uma configuração do Snapper. No LVM, é necessário especificar o sistema de arquivos com `--fstype=lvm(`*`SISTEMADEARQUIVOS`*`)`. Os dados ext3 e XFS são suportados, portanto `ext3` ou `xfs` são valores válidos para *`SISTEMADEARQUIVOS`*. Exemplo:

```
snapper -c lvm create-config --fstype="lvm(xfs)" /thin_lvm
```

É possível ajustar essa configuração de acordo com as suas necessidades conforme descrito na Seção 4.2.3.1, "Ajustando o arquivo de configuração" (p 38). Agora, é possível usar o Snapper para criar e gerenciar instantâneos, restaurar arquivos e desfazer mudanças, conforme descrito anteriormente.

5 Acesso remoto com VNC

O VNC (Virtual Network Computing) permite controlar um computador remoto por uma área de trabalho gráfica (ao contrário do acesso remoto a shell). O VNC é independente de plataforma e permite acessar a máquina remota de qualquer sistema operacional.

O SUSE Linux Enterprise Desktop suporta dois tipos diferentes de sessões VNC: sessões únicas, que permanecem “ativas” enquanto a conexão VNC do cliente está ativada, e sessões persistentes, que permanecem “ativas” até serem explicitamente terminadas.

NOTA: Tipos de sessão

Uma máquina é capaz de oferecer ambos os tipos de sessões simultaneamente em portas diferentes, mas uma sessão aberta não pode ser convertida de um tipo em outro.

5.1 Sessões VNC únicas

Uma sessão única é iniciada por um cliente remoto. Ela inicia uma tela gráfica de login no servidor. Desse modo, você pode escolher o usuário que inicia a sessão e, se suportado pelo gerenciador de login, o ambiente de área de trabalho. Após terminar a conexão do cliente para essa sessão VNC, todos os aplicativos iniciados nessa sessão também serão terminados. Sessões VNC únicas não podem ser compartilhadas, mas é possível ter várias sessões em um único host ao mesmo tempo.

Procedimento 5.1 *Habilitando sessões VNC únicas*

1 Inicie o *YaST* > *Serviços de Rede* > *Administração Remota (VNC)*.

2 Marque *Permitir Administração Remota*.

3 Se necessário, marque também *Abrir Porta no Firewall* (por exemplo, quando a interface de rede estiver configurada para ficar na Zona Externa). Se você tem mais de uma interface de rede, restrinja a abertura de portas no firewall a uma interface específica em *Detalhes do Firewall*.

4 Confirme as suas configurações clicando em *Concluir*.

5 Caso nem todos os pacotes necessários já estejam disponíveis, aprove a instalação dos pacotes ausentes.

NOTA: Configurações disponíveis

A configuração padrão no SUSE Linux Enterprise Desktop confere às sessões uma resolução de 1024 x 768 pixels com profundidade de cores de 16 bits. As sessões estão disponíveis nas portas `5901` para viewers VNC “regulares” (equivalente à exibição VNC `1`) e na porta `5801` para browsers da Web.

É possível disponibilizar outras configurações em portas diferentes. Pergunte ao administrador do sistema.

Os números de exibição VNC e os números de exibição X são independentes nas sessões únicas. Um número de exibição VNC é atribuído manualmente a todas as configurações suportadas pelo servidor (:1 no exemplo acima). Sempre que uma sessão VNC é iniciada com uma das configurações, ela recebe automaticamente um número de exibição X livre.

5.1.1 Iniciando uma sessão VNC única

Para iniciar uma sessão VNC única, é preciso instalar um viewer VNC na máquina cliente. O viewer padrão nos produtos SUSE Linux é o `vncviewer`, incluído no pacote `tightvnc`. É possível também ver uma sessão VNC pelo browser da Web e por um applet Java.

Para iniciar seu viewer VNC e iniciar uma sessão com a configuração padrão do servidor, use o comando:

```
vncviewer jupiter.example.com:1
```

Em vez do número de exibição do VNC, você também pode especificar o número da porta com dois-pontos duplos:

```
vncviewer jupiter.example.com::5901
```

Se preferir, use um browser da Web compatível com Java para ver a sessão VNC digitando o seguinte URL: `http://jupiter.example.com:5801`

5.1.2 Configurando sessões VNC únicas

Você poderá ignorar esta seção se não precisar nem desejar modificar a configuração padrão.

As sessões VNC únicas são iniciadas pelo daemon `xinetd`. Um arquivo de configuração está localizado em `/etc/xinetd.d/vnc`. Por padrão, ele oferece seis blocos de configuração: três para viewers VNC (`vnc1` a `vnc3`) e três para atender a um applet Java (`vnchttpd1` a `vnchttpd3`). Por padrão, apenas `vnc1` e `vnchttpd1` estão ativos.

Para ativar uma configuração, comente a linha `disable = yes` com o caractere `#` na primeira coluna ou remova totalmente essa linha. Para desativar uma configuração, remova o comentário ou adicione a linha.

O servidor `Xvnc` pode ser configurado pela opção `server_args`. Consulte `Xnvc --help` para obter a lista de opções.

Ao adicionar configurações padrão, certifique-se de que elas não usem portas já em uso por outras configurações, outros serviços ou sessões VNC persistentes existentes no mesmo host.

Ative as mudanças na configuração digitando o seguinte comando:

```
rcxinetd reload
```

IMPORTANTE: Firewall e portas VNC

Ao ativar a Administração Remota conforme descrito no Procedimento 5.1, “Habilitando sessões VNC únicas” (p 52), as portas `5801` e `5901` são abertas no firewall. Se a interface de rede que atende às sessões VNC for protegida por firewall, será necessário abrir manualmente as respectivas portas ao ativar portas adicionais para as sessões VNC. Consulte o Chapter 15, *Masquerading and Firewalls* (↑*Security Guide*) para obter instruções.

5.2 Sessões VNC persistentes

Uma sessão VNC persistente é iniciada no servidor. A sessão e todos os aplicativos iniciados nessa sessão são executados independentemente das conexões do cliente até a sessão ser terminada.

É possível acessar uma sessão persistente de vários clientes ao mesmo tempo. Isso é ideal para fins de demonstração em que um cliente tem acesso total, e todos os outros têm acesso apenas exibição. Outro cenário de uso são treinamentos em que o instrutor pode precisar acessar a área de trabalho do aluno. Mas, na maioria das vezes, você possivelmente não vai querer compartilhar sua sessão VNC.

Ao contrário das sessões únicas que iniciam um gerenciador de exibição, uma sessão persistente inicia uma área de trabalho pronta para funcionar executada como o usuário que iniciou a sessão VNC.

O acesso às sessões persistentes é protegido por dois tipos de senhas possíveis:

- uma senha regular que permite acesso total ou
- uma senha opcional apenas exibição que permite acesso não interativo (apenas exibição).

Uma sessão pode ter várias conexões de cliente de ambos os tipos de uma só vez.

Procedimento 5.2 *Iniciando uma sessão VNC persistente*

1 Abra um shell e verifique se você está conectado como o usuário proprietário da sessão VNC.

2 Se a interface de rede que atende às sessões VNC for protegida por firewall, será necessário abrir manualmente a porta usada pela sessão no firewall. Se você iniciar várias sessões, poderá também abrir uma faixa de portas. Consulte o Chapter 15, *Masquerading and Firewalls* (↑*Security Guide*) para obter os detalhes sobre como configurar o firewall.

   O `vncserver` usa as portas `5901` para exibição `:1`, `5902` para exibição `:2`, e assim por diante. Para sessões persistentes, a exibição VNC e a exibição X geralmente têm o mesmo número.

3 Para iniciar uma sessão com resolução de 1024 x 769 pixels e profundidade de cores de 16 bits, digite o seguinte comando:

```
vncserver -geometry 1024x768 -depth 16
```

   O comando `vncserver` escolhe um número de exibição não usado quando nenhum número é especificado e imprime essa escolha. Consulte `man 1 vncserver` para ver mais opções.

Quando você executa o `vncviewer` pela primeira vez, ele pede uma senha para acesso total à sessão. Se necessário, forneça também uma senha de acesso apenas exibição à sessão.

A(s) senha(s) inserida(s) aqui também será(ão) usada(s) em sessões futuras iniciadas pelo mesmo usuário. Elas podem ser modificadas com o comando `vncpasswd`.

IMPORTANTE: Considerações sobre segurança

Verifique se está usando senhas avançadas de tamanho significativo (oito ou mais caracteres). Não compartilhe essas senhas.

As conexões VNC não são criptografadas, portanto, quem conseguir detectar a(s) rede(s) entre as duas máquinas poderá ler a senha quando ela for transferida no início de uma sessão.

Para terminar a sessão, encerre o ambiente de área de trabalho executado na sessão VNC pelo viewer do VNC, da mesma forma que você encerra uma sessão X local regular.

Se preferir terminar a sessão manualmente, abra um shell no servidor VNC e certifique-se de estar conectado como o usuário que possui a sessão VNC que deseja terminar.

Execute o seguinte comando para terminar a sessão em execução na exibição `:1`: `vncserver -kill :1`

5.2.1 Conectando-se a uma sessão VNC persistente

Para conectar-se a uma sessão VNC persistente, é preciso instalar o viewer do VNC. O viewer padrão nos produtos SUSE Linux é o `vncviewer`, incluído no pacote `tightvnc`. É possível também ver uma sessão VNC pelo browser da Web e por um applet Java.

Para iniciar o viewer do VNC e conectar-se à exibição `:1` do servidor VNC, use o comando

```
vncviewer jupiter.example.com:1
```

Em vez do número de exibição do VNC, você também pode especificar o número da porta com dois-pontos duplos:

```
vncviewer jupiter.example.com::5901
```

Se preferir, use um browser da Web compatível com Java para ver a sessão VNC digitando o seguinte URL: `http://jupiter.example.com:5801`

5.2.2 Configurando sessões VNC persistentes

É possível configurar as sessões VNC persistentes editando `$HOME/.vnc/xstartup`. Por padrão, esse script shell inicia um `xterm` e o Gerenciador de Janelas `twm`. Para iniciar o GNOME ou o KDE, substitua a linha que começa com `twm` pela seguinte:

```
/usr/bin/gnome     # GNOME
/usr/bin/startkde  # KDE
```

NOTA: Uma configuração para cada usuário

Sessões VNC persistentes são configuradas em uma única configuração por usuário. Todas as diversas sessões iniciadas por um usuário utilizarão os mesmos arquivos de inicialização e senha.

Configuração do GNOME para administradores

6

Este capítulo introduz as opções de configuração do GNOME que os administradores podem usar para definir ajustes em todo o sistema, como personalização de menus, instalação de temas, configuração de fontes, mudança dos aplicativos preferidos e bloqueio de recursos.

Essas opções de configuração estão armazenadas no sistema GConf. Acesse o sistema GConf usando ferramentas como a interface de linha de comando `gconftool-2` ou a interface gráfica do usuário `gconf-editor`.

6.1 O sistema GConf

A área de trabalho do GNOME gerencia sua própria configuração com o GConf. Trata-se de um banco de dados ou registro de estrutura hierárquica, no qual o usuário pode mudar suas próprias configurações e o administrador do sistema pode definir valores padrão ou obrigatórios para todos os usuários. Especifique caminhos de acesso para acessar as configurações do GConf, como `/desktop/gnome/background/picture_filename`; por exemplo, essa é a chave que armazena o nome de arquivo da imagem de fundo da área de trabalho.

Use o `gconf-editor` gráfico se quiser navegar por todas as opções de forma conveniente. Para obter uma descrição resumida sobre o uso do gconf-editor, consulte a Seção 6.1.1, "O gconf-editor gráfico" (p 58). Se você precisar de uma solução baseada em scripts, consulte a Seção 6.1.2, "Interface da linha de comando gconftool-2" (p 59).

ATENÇÃO: caixas de diálogo do Centro de Controle GNOME

O acesso direto ao Sistema Gconf, se feito de forma descuidada, pode fazer o sistema ficar inutilizável.

Para os usuários inexperientes que queiram ajustar apenas alguns recursos comuns da área de trabalho, recomenda-se usar as caixas de diálogo de configuração do Centro de Controle GNOME. Para iniciar o Centro de Controle GNOME, clique em *Computador* > *Centro de Controle*. Para obter mais informações, consulte a Seção "Centro de Controle" (Capítulo 3, *Personalizando suas configurações*, ↑*Guia do Usuário do GNOME*).

6.1.1 O gconf-editor gráfico

O gconf-editor permite navegar nas configurações do GConf e mudá-las de forma interativa. Para iniciar o gconf-editor na tela padrão da *janela Configurações*, clique em *Computador* > *Mais Aplicativos* e, no grupo *Sistema*, clique em *Editor de Configuração do GNOME*.

Por padrão, os usuários podem mudar as configurações de suas próprias áreas de trabalho, e o administrador pode preparar configurações para especificar valores padrão ou obrigatórios. Por exemplo, se você quiser habilitar o recurso de *interrupção de digitação* como obrigatório para todos os usuários, proceda da seguinte maneira:

1. Inicie o `gconf-editor` como `root` na linha de comando.

2. No painel de árvore à esquerda, expanda `/desktop/gnome/typing_break`.

3. Clique o botão direito do mouse em *habilitado* e selecione *Definir como Obrigatório*. Depois disso, você poderá gerenciar este recurso.

4. Abra a janela *Configurações obrigatórias* clicando em *Arquivo* > *Nova Janela Obrigatória*.

5. No painel de árvore da janela *Configurações obrigatórias*, expanda `/desktop/gnome/typing_break` e clique em *habilitado*.

6. Feche a janela para gravar as configurações clicando em *Arquivo* > *Fechar Janela*.

Para obter mais informações sobre o gconf-editor, consulte o Manual do Editor de Configurações em http://library.gnome.org/users/gconf-editor/stable/.

6.1.2 Interface da linha de comando gconftool-2

Para mudar as configurações a partir da linha de comando ou de dentro dos scripts, use gconftool-2. Veja alguns exemplos a seguir:

Como root, use o seguinte comando para listar os valores de todas as chaves:

```
gconftool-2 --recursive-list /
```

Se tiver interesse em apenas um subconjunto, especifique um caminho de acesso como /desktop/gnome/typing_break:

```
gconftool-2 --recursive-list /desktop/gnome/typing_break
```

Para listar as configurações obrigatórias:

```
gconftool-2 --recursive-list \
  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory /
```

Para definir uma configuração obrigatória, como typing_break:

```
gconftool-2 \
  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \
  --type bool \
  --set /desktop/gnome/typing_break/enabled true
```

Para cancelar a definição de uma configuração obrigatória:

```
gconftool-2 \
  --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory \
  --unset /desktop/gnome/typing_break/enabled
```

Para acessar as configurações padrão, use /etc/gconf/gconf.xml.default.

Para obter mais informações sobre gconftool-2, consulte o Guia de Administração do Sistema do Ambiente de Trabalho GNOME, seção Ferramenta de Linha de Comando GConf em http://help.gnome.org/admin/system-admin-guide/2

.32/gconf-6.html.en e a página de manual de gconftool-2 (man gconftool-2).

6.2 Personalizado o menu principal, o painel e o browser de aplicativos

Controle os itens padrão mostrados em várias seções do menu principal (*Computador*) personalizado os seguintes arquivos:

- **/usr/share/gnome-main-menu/applications.xbel:** lista dos aplicativos padrão favoritos.
- **/usr/share/gnome-main-menu/documents.xbel:** lista dos documentos padrão favoritos.
- **/usr/share/gnome-main-menu/system-items.xbel:** itens mostrados na seção do sistema.

Com o gconf-editor, você pode personalizar o número de itens exibidos:

- **/desktop/gnome/applications/main-menu/file-area/min_recent_items:** número mínimo de itens recentes.
- **/desktop/gnome/applications/main-menu/file-area/max_total_items:** número máximo do total de itens.

Você pode personalizar o browser de aplicativos de várias maneiras, por exemplo, seu comportamento quando os usuários iniciam itens ou o número de itens exibidos na categoria *Novos Aplicativos*. Procure as chaves /desktop/gnome/applications/main-menu/ab_* com o gconf-editor.

Para obter mais informações, consulte a seção Personalizar Menus no Guia de Administração do Sistema do Ambiente de Trabalho GNOME em https://help.gnome.org/admin/system-admin-guide/2.32/menustructure-0.html.en.

6.3 Iniciando aplicativos automaticamente

Para iniciar aplicativos automaticamente no GNOME, use um dos seguintes métodos:

- **Para executar aplicativos para cada usuário:** coloque os arquivos `.desktop` em `/usr/share/gnome/autostart`.

- **Para executar aplicativos para um único usuário:** coloque os arquivos `.desktop` em `~/.config/autostart`.

Para desabilitar um aplicativo que é iniciado automaticamente, adicione `X-Autostart-enabled=false` ao arquivo `.desktop`.

6.4 Montando automaticamente e gerenciando dispositivos de mídia

O Nautilus (`nautilus`) monitora eventos relacionados a volume e responde com uma política especificada pelo usuário. Você pode usar o Nautilus para montar automaticamente as unidades de hot plug e a mídia removível inserida, executar programas automaticamente e reproduzir CDs de áudio ou DVDs de vídeo. O Nautilus também pode importar automaticamente fotos de uma câmera digital.

Os administradores do sistema podem definir padrões para todo o sistema. Para obter mais informações, consulte a Seção 6.5, “Mudando os aplicativos preferenciais” (p 61).

6.5 Mudando os aplicativos preferenciais

Para mudar os aplicativos preferenciais dos usuários, edite `/etc/gnome_defaults.conf`. Mais dicas são encontradas neste arquivo.

Após editar o arquivo, execute `SuSEconfig --module glib2`.

Para obter mais informações sobre tipos MIME, consulte http://www.freedesktop.org/Standards/shared-mime-info-spec.

6.6 Gerenciando perfis com o Sabayon

Sabayon é uma ferramenta de administração do sistema para criar e aplicar perfis do ambiente de área de trabalho. Perfil de área de trabalho é uma coleção de restrições e configurações padrão que podem ser aplicadas a usuários individuais ou a grupos de usuários. O Sabayon permite editar os padrões e chaves obrigatórias do GConf usando uma ferramenta gráfica.

A definição de perfil é feita por meio de uma sessão gráfica semelhante à sessão executada por um usuário, porém dentro de uma janela da área de trabalho. Você pode mudar as propriedades (como o segundo plano da área de trabalho, as barras de ferramentas e os applets disponíveis) normalmente. O Sabayon também detecta mudanças nas configurações padrão de quase todos os aplicativos.

Os arquivos ou documentos que ficam no diretório pessoal simulado ou na área de trabalho são incluídos no perfil concluído. Entre eles, muitos bancos de dados específicos de aplicativos, como as anotações do Tomboy. Com o uso desse mecanismo, é fácil fornecer anotações introdutórias ou modelos facilmente acessíveis aos novos usuários.

Um perfil de usuário pode herdar suas configurações de um perfil pai, anulando ou adicionando valores específicos. Isso habilita conjuntos de configurações hierárquicos. Por exemplo, você pode definir um perfil Empregado e derivar dele os perfis Artista e Garantia de Qualidade.

Além de fornecer padrões, o Sabayon também pode bloquear configurações. Esse recurso protege a configuração contra as mudanças de usuários. Por exemplo, você pode especificar que o segundo plano da área de trabalho não pode ser mudado para algo que não seja o padrão fornecido por você. Isso evita violações casuais das configurações, o que reduz o número de chamadas ao suporte técnico, além de habilitar ambientes tipo quiosque. Contudo, ele não fornece segurança absoluta e não deve ser usado para tal.

O Sabayon também fornece uma lista de configurações para aplicativos e elementos genéricos da interface do usuário que possuem suporte interno de bloqueio, incluindo

o OpenOffice.org e o painel do GNOME. Por exemplo, o painel pode ser configurado de modo a permitir a inclusão apenas de applets específicos e impedir a mudança de seu local ou tamanho na tela. Da mesma maneira, os itens do menu Gravar podem ser desabilitados para todos os aplicativos que o utilizam, impedindo que os usuários gravem documentos.

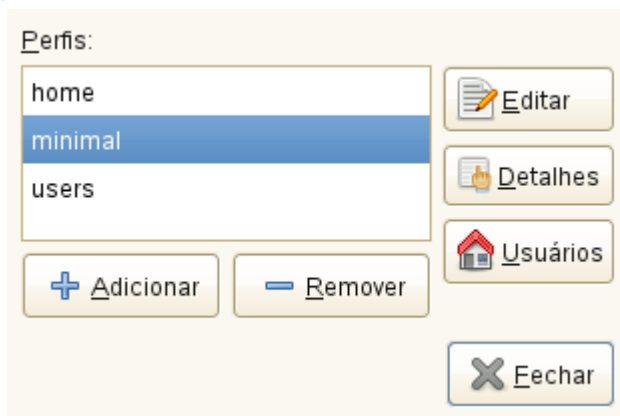
Os perfis podem ser transferidos para outros computadores. Eles ficam em `/etc/desktop-profiles/`, sendo que cada perfil é gravado em um arquivo ZIP separado.

6.6.1 Criando um perfil

Os perfis são gravados em arquivos ZIP localizados em `/etc/desktop-profiles`. Cada perfil que você grava é armazenado em um arquivo ZIP separado, como *`nome do perfil`*`.zip`. Você pode copiar ou mover os perfis para outros computadores.

1 Clique em *Computador* > *Mais Aplicativos* > *System* > *Editor de Perfil de Usuário*.

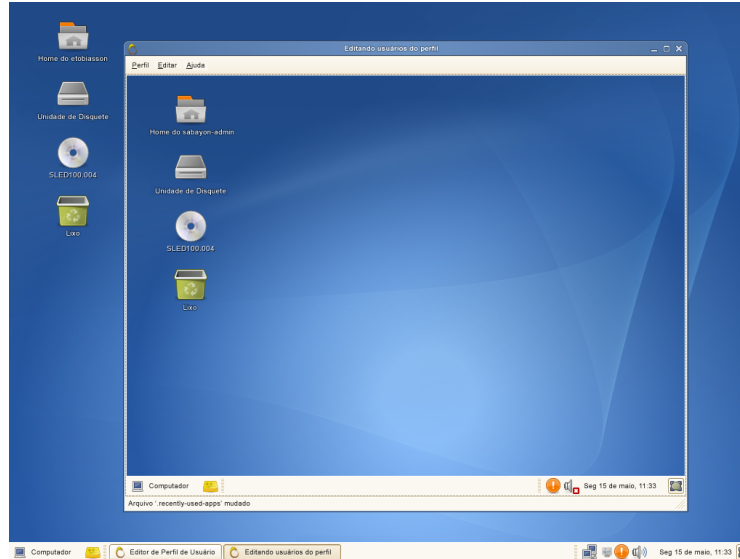
2 Se você não estiver conectado como `root`, digite a senha do `root` e clique em *Continuar*.

Figura 6.1 *Sabayon: Editor de Perfil de Usuário*

3 Clique em *Adicionar*.

4 Especifique um nome para o perfil e clique em *Adicionar*.

5 Selecione o perfil e clique em *Editar*.

Uma nova sessão da área de trabalho é aberta em uma janela do Xnest.

Figura 6.2 *Sabayon: nova janela do Xnest*

6 Na janela do Xnest, faça as mudanças nas configurações de sua escolha.

Cada configuração que você muda aparece na janela do Xnest.

Você pode optar por tornar obrigatórias todas as configurações (clicando em *Editar* > *Assegurar o Uso Obrigatório*), ignorar uma configuração (clicando em *Editar* > *Mudanças* > *Ignorar*) ou tornar uma configuração o padrão (não selecionando *Ignorar* nem *Obrigatório*).

7 Para bloquear as configurações para os usuários, clique em *Editar* > *Bloqueio* na janela do Xnest.

Você pode escolher uma destas opções:

Geral: permite desabilitar a linha de comando, a impressão, a configuração de impressão e o recurso de gravação em disco.

Painel: permite bloquear os painéis, desabilitar o fechamento forçado, desabilitar o bloqueio de tela, desabilitar o logout e desabilitar qualquer applet da lista *Desabilitar Applets*.

OpenOffice.org: permite definir o nível de segurança de macro para os documentos do OpenOffice.org, opções de carregamento e gravação, e opções da interface do usuário.

8 Para gravar o perfil, clique em *Perfil* > *Gravar*.

   O perfil é gravado em `/etc/desktop-profiles`.

9 Clique em *Perfil* > *Sair* para fechar a janela do Xnest e clique em *Fechar* para sair do Sabayon.

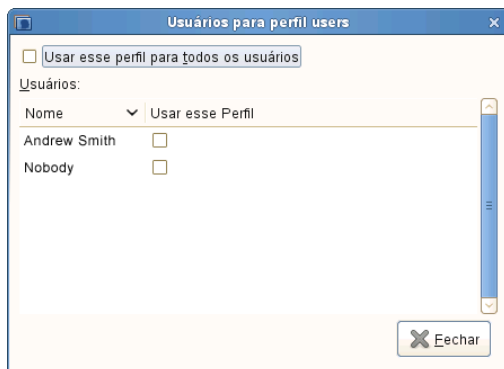
6.6.2 Aplicando um perfil

Você pode aplicar um perfil a usuários individuais ou a todos os usuários em uma estação de trabalho.

1 Clique em *Computador* > *Mais Aplicativos* > *System* > *Editor de Perfil de Usuário*.

2 Se você não estiver conectado como `root`, digite a senha do `root` e clique em *Continuar*.

3 Selecione o perfil que deseja aplicar e clique em *Usuários*.

Figura 6.3 *Sabayon: selecionando usuários*

4 Selecione os usuários que usarão esse perfil.

Para aplicar o perfil a todos os usuários da estação de trabalho, clique em *Usar esse perfil para todos os usuários*.

5 Clique em *Fechar*.

6.7 Adicionando modelos de documentos

Para disponibilizar gabaritos de documentos aos usuários, insira-os no diretório `Templates` no diretório pessoal de um usuário. Isso pode ser feito manualmente para cada usuário, copiando-se os arquivos para `~/Templates`, ou para todo o sistema, adicionando-se um diretório `Templates` com documentos a `/etc/skel` antes que o usuário seja criado.

Um usuário cria um novo documento a partir de um modelo clicando o botão direito do mouse na área de trabalho e selecionando *Criar Documento*.

6.8 Recursos de bloqueio da área de trabalho

Às vezes, convém remover ou desabilitar recursos da área de trabalho ou o acesso do usuário ao sistema operacional subjacente. O GNOME oferece recursos de bloqueio capazes de mudar a área de trabalho conforme a necessidade. Tecnicamente, você define chaves GConf para implementarem essas mudanças.

Por exemplo, se você abrir o gconf-editor, verá as chaves de bloqueio do menu principal em `/desktop/gnome/applications/main-menu/lock-down/application_browser_link_visible`. Esse local também contém as descrições de todas as chaves. Outras chaves de bloqueio:

/desktop/gnome/lockdown/disable_command_line
: Se definida, os terminais não são mostrados no menu principal nem no Browser de Aplicativos.

/apps/panel/global/disable_log_out

/apps/panel/global/disable_lock_screen
Se definidas, o menu principal não mostra esses itens.

As chaves de bloqueio do Firefox estão em /apps/firefox/lockdown.

Para obter mais informações, consulte o “Desktop Administrators' Guide to GNOME Lockdown and Preconfiguration” (Guia do Administrador da Área de Trabalho para Bloqueio e Pré-configuração do GNOME), escrito por Sayamindu Dasgupta: http://library.gnome.org/admin/deployment-guide/.

6.9 Para obter mais informações

Para obter mais informações, consulte http://library.gnome.org/admin/.

Gerenciando software com ferramentas de linha de comando

7

Este capítulo descreve o Zypper e o RPM, duas ferramentas de linha de comando para gerenciar software. Para obter a definição da terminologia usada neste contexto (por exemplo, `repositório`, `patch` ou `atualização`), consulte a Section “Definition of Terms” (Chapter 6, *Installing or Removing Software*, ↑*Deployment Guide*).

7.1 Usando o zypper

O zypper é um gerenciador de pacotes de linha de comando para instalar, atualizar e remover pacotes, bem como para gerenciar repositórios. A sintaxe do zypper é semelhante à do rug. Ao contrário do rug, o zypper não requer que o daemon zmd seja executado nos bastidores. Para obter mais informações sobre compatibilidade com o rug, consulte `man zypper`, seção “COMPATIBILIDADE COM O RUG”. Ele é especialmente útil para realizar tarefas de gerenciamento remoto de software ou gerenciar software de scripts de shell.

7.1.1 Uso geral

A sintaxe geral do zypper é:

```
zypper [global-options]command[command-options][arguments] ...
```

Os componentes entre colchetes não são obrigatórios. A maneira mais simples de executar o zypper é digitar seu nome seguido de um comando. Por exemplo, para aplicar todos os patches necessários ao sistema, digite:

```
zypper patch
```

Além disso, você pode escolher dentre uma ou mais opções globais, digitando-as antes do comando. Por exemplo, `--non-interactive` significa executar o comando sem perguntar nada (aplicando as respostas padrão automaticamente):

```
zypper --non-interactive patch
```

Para usar as opções específicas de um comando em particular, digite-as logo após o comando. Por exemplo, `--auto-agree-with-licenses` significa aplicar todos os patches necessários ao sistema sem solicitar confirmação de nenhuma licença (eles serão aceitos automaticamente):

```
zypper patch --auto-agree-with-licenses
```

Alguns comandos requerem um ou mais argumentos. Ao usar o comando install, por exemplo, é preciso especificar o(s) pacotes(s) a instalar:

```
zypper install mplayer
```

Algumas opções também requerem um argumento. O comando a seguir lista todos os padrões conhecidos:

```
zypper search -t pattern
```

Você pode combinar todos os anteriores. Por exemplo, o comando a seguir instala os pacotes `mplayer` e `amarok` do repositório `factory` durante o modo verboso:

```
zypper -v install --from factory mplayer amarok
```

A opção `--from` trata de manter todos os repositórios habilitados (para resolução de dependências) enquanto solicita o pacote do repositório especificado.

Quase todos os comandos zypper possuem uma opção `dry-run` que simula o comando indicado. Ela pode ser usada para fins de teste.

```
zypper remove --dry-run MozillaFirefox
```

O Zypper suporta a opção global `--userdata` *`string`* para fins de identificação da transação. A string definida pelo usuário é passada para os registros de histórico do Zypper em `/var/log/zypp/history` e no Snapper.

```
zypper --userdata string patch
```

7.1.2 Instalando e removendo software com o zypper

Para instalar ou remover pacotes, use os seguintes comandos:

```
zypper install package_name
zypper remove package_name
```

O zypper conhece várias maneiras de tratar pacotes para os comandos install e remove:

pelo nome exato do pacote (e número da versão)

```
zypper install MozillaFirefox
```

ou

```
zypper install MozillaFirefox-3.5.3
```

pelo álias do repositório e pelo nome do pacote

```
zypper install mozilla:MozillaFirefox
```

onde `mozilla` é o álias do repositório a partir do qual instalar.

pelo nome do pacote usando curingas
O comando a seguir instalará todos os pacotes cujos nomes começam com “Moz”. Use-o com cuidado, principalmente ao remover pacotes.

```
zypper install 'Moz*'
```

por recurso
Por exemplo, para instalar um módulo perl sem saber o nome do pacote, os recursos podem ser convenientes:

```
zypper install 'perl(Time::ParseDate)'
```

por recurso e/ou arquitetura e/ou versão
Juntamente com um recurso, você pode especificar uma arquitetura (como `i586` ou `x86_64`) e/ou uma versão. A versão deve ser precedida por um operador: < (menor que), <= (menor que ou igual), = (igual), >= (maior que ou igual), > (maior que).

```
zypper install 'firefox.x86_64'
zypper install 'firefox>=3.5.3'
zypper install 'firefox.x86_64>=3.5.3'
```

por caminho para o arquivo RPM
Você também pode especificar um local ou caminho remoto para um pacote:

```
zypper install /tmp/install/MozillaFirefox.rpm
zypper install
http://download.opensuse.org/repositories/mozilla/SUSE_Factory/x86_64/MozillaFirefox-3.5.3-1.3.x86_64.rpm
```

Para instalar e remover pacotes simultaneamente, use os modificadores `+/-`. Para instalar o `emacs` e remover o `vim` simultaneamente, use:

```
zypper install emacs -vim
```

Para remover o `emacs` e instalar o `vim` simultaneamente, use:

```
zypper remove emacs +vim
```

Para impedir que o nome do pacote iniciado por `-` seja interpretado como uma opção de comando, use-o sempre como segundo argumento. Se isso não for possível, preceda-o com `--`:

```
zypper install -emacs +vim       # Wrong
zypper install vim -emacs        # Correct
zypper install -- -emacs +vim    # same as above
zypper remove emacs +vim         # same as above
```

Para (com determinado pacote) remover automaticamente qualquer pacote desnecessário após remover o pacote especificado, use a opção `--clean-deps`:

```
rm package_name --clean-deps
```

Por padrão, o zypper solicita uma confirmação antes de instalar ou remover um pacote selecionado, ou quando ocorre um problema. Você pode anular esse comportamento usando a opção `--non-interactive`. Essa opção deve ser inserida antes do comando real (`install`, `remove` e `patch`), conforme mostrado a seguir:

```
zypper --non-interactive install package_name
```

Essa opção permite o uso do zypper em scripts e tarefas cron.

ATENÇÃO: não remova pacotes de sistema obrigatórios

Não remova pacotes como `glibc`, `zypper`, `kernel` ou similares. Esses pacotes são obrigatórios para o sistema e, se removidos, podem fazer o sistema ficar instável ou parar de funcionar de vez.

7.1.2.1 Instalando ou fazendo download dos pacotes de origem

Se desejar instalar o pacote de origem de um pacote, use:

```
zypper source-install package_name
```

Esse comando também instalará as dependências de compilação do pacote especificado. Se não quiser isso, adicione o switch `-D`. Para instalar apenas as dependências de compilação, use `-d`.

```
zypper source-install -D package_name # source package only
zypper source-install -d package_name # build dependencies only
```

Naturalmente isso só funcionará se o repositório com os pacotes de origem estiver habilitado na sua lista de repositórios (ele é adicionado por padrão, mas não habilitado). Consulte a Seção 7.1.5, “Gerenciando repositórios com o zypper” (p 81) para obter os detalhes sobre o gerenciamento de repositórios.

Uma lista de todos os pacotes de origem disponíveis nos seus repositórios pode ser obtida com:

```
zypper search -t srcpackage
```

É possível também fazer download dos pacotes de origem para todos os pacotes instalados em um diretório local. Para fazer download dos pacotes de origem, use:

```
zypper source-download
```

O diretório de download padrão é `/var/cache/zypper/source-download`. Você pode mudá-lo usando a opção `--directory`. Para mostrar apenas os pacotes ausentes ou incorretos sem fazer download nem apagar nada, use a opção `--status`. Para apagar pacotes de origem incorretos, use a opção `--delete`. Para desabilitar a exclusão, use a opção `--no-delete`.

7.1.2.2 Utilitários

Para verificar se todas as dependências ainda são atendidas e para reparar dependências ausentes, use:

```
zypper verify
```

Além das dependências que precisam ser atendidas, alguns pacotes “recomendam” outros pacotes. Esses pacotes recomendados são instalados apenas quando estão realmente disponíveis e são instaláveis. Caso os pacotes recomendados fiquem disponíveis após a instalação do pacote que os recomendou (adicionando outros pacotes ou hardware), use o seguinte comando:

```
zypper install-new-recommends
```

Esse comando é muito útil após conectar uma webcam ou um dispositivo WLAN. Ele instala drivers para o dispositivo e software relacionado, se disponíveis. Os drivers e o software relacionado serão instaláveis se determinadas dependências de hardware forem atendidas.

7.1.3 Atualizando software com o zypper

Existem três maneiras diferentes de atualizar o software usando o zypper: instalando patches, instalando uma versão nova de um pacote ou atualizando a distribuição inteira. Para executar a última maneira, usa-se o comando `zypper dist-upgrade`, abordado na Seção 7.1.4, “Upgrade de distribuição com o zypper” (p 78).

7.1.3.1 Instalando patches

Para instalar todos os patches lançados oficialmente que se aplicam ao seu sistema, execute:

```
zypper patch
```

Nesse caso, todos os patches disponíveis em seus repositórios são verificados quanto à sua relevância e instalados, se necessário. Após o registro de sua instalação do SUSE Linux Enterprise Desktop, um repositório de atualização oficial contendo os patches será adicionado ao seu sistema. O comando acima é tudo o que você deve digitar para aplicá-los quando necessário.

O zypper conhece três comandos diferentes para consultar a disponibilidade dos patches:

`zypper patch-check`
: Lista o número de patches necessários (patches que se aplicam ao seu sistema e ainda não estão instalados)

```
~ # zypper patch-check
Loading repository data...
Reading installed packages...
5 patches needed (1 security patch)
```

`zypper list-patches`
: Lista todos os patches necessários (patches que se aplicam ao seu sistema e ainda não estão instalados)

```
~ # zypper list-patches
Loading repository data...
Reading installed packages...

Repository                         | Name      | Version | Category | Status
-----------------------------------+-----------+---------+----------+-------
Updates for openSUSE 11.3 11.3-1.82 | lxsession | 2776    | security | needed
```

`zypper patches`
: Lista todos os patches disponíveis para o SUSE Linux Enterprise Desktop, independentemente de já estarem instalados ou de se aplicarem à sua instalação.

Também é possível listar e instalar todos os patches relevantes a problemas específicos. Para listar patches específicos, use o comando `zypper list-patches` com as seguintes opções:

`--bugzilla[=`*`número`*`]`
: Lista todos os patches necessários para problemas do Bugzilla. Opcionalmente, você pode inserir um número de bug para listar apenas os patches para esse bug específico.

`--cve[=`*`número`*`]`
: Lista todos os patches necessários para problemas do CVE (Common Vulnerabilities and Exposures) ou apenas os patches correspondentes a determinado número de CVE, se especificado. Por padrão, apenas os patches não aplicados aparecem na lista. Use `-a` para listar tudo.

Para instalar um patch para um problema específico do Bugzilla ou do CVE, use os seguintes comandos:

```
zypper patch --bugzilla=number
```

ou

```
zypper patch --cve=number
```

Por exemplo, para instalar um patch de segurança com o número do CVE `CVE-2010-2713`, execute:

```
zypper patch --cve=CVE-2010-2713
```

7.1.3.2 Instalando atualizações

Se um repositório contém apenas pacotes novos, mas não fornece patches, `zypper patch` não surte nenhum efeito. Para atualizar todos os pacotes instalados com versões disponíveis mais novas, use:

```
zypper update
```

Para atualizar pacotes individuais, especifique o pacote com o comando update ou install:

```
zypper update package_name
zypper install package_name
```

Uma lista de todos os novos pacotes instaláveis pode ser obtida pelo comando:

```
zypper list-updates
```

Observe que esse comando apenas lista os pacotes correspondentes aos seguintes critérios:

- têm os mesmo fornecedor que o pacote já instalado,
- são fornecidos por repositórios com pelo menos a mesma prioridade que o pacote já instalado,
- são instaláveis (todas as dependências foram atendidas).

Uma lista de *todos* os novos pacotes disponíveis (sejam instaláveis ou não) pode ser obtida com:

```
zypper list-updates --all
```

Para descobrir o motivo pelo qual um novo pacote não pode ser instalado, basta usar o comando `zypper install` ou `zypper update` conforme descrito acima.

7.1.3.3 Fazendo upgrade para uma nova versão de produto

Para fazer upgrade da instalação para uma nova versão do produto (por exemplo, do SUSE Linux Enterprise Server 11 para o SUSE Linux Enterprise Server 11 SP1 com facilidade, ajuste primeiro os repositórios para corresponder aos repositórios atuais do SUSE Linux Enterprise Desktop. Para obter informações detalhadas, consulte a Seção 7.1.5, "Gerenciando repositórios com o zypper" (p 81). Em seguida, use o comando `zypper dist-upgrade` com os repositórios necessários. Esse comando garante que todos os pacotes serão instalados a partir dos repositórios atualmente habilitados. Para obter instruções detalhadas, consulte Seção 7.1.4, "Upgrade de distribuição com o zypper" (p 78).

Para restringir o upgrade de distribuição aos pacotes de determinado repositório e, ao mesmo tempo, considerar os outros repositórios para atender às dependências, use a opção `--from` e especifique o repositório por seu álias, número ou URI.

NOTA: diferenças entre `zypper update` e `zypper dist-upgrade`

Escolha `zypper update` para atualizar os pacotes com as versões mais recentes disponíveis para a sua versão do produto e manter a integridade do sistema. `zypper update` obedecerá às seguintes regras:

nenhuma mudança de fornecedor
nenhuma mudança de arquitetura
nenhum downgrade
manter pacotes instalados

Ao executar `zypper dist-upgrade`, todos os pacotes serão instalados dos repositórios habilitados. Como essa regra tem uso obrigatório assegurado, os pacotes podem mudar de fornecedor ou arquitetura ou até sofrer downgrade. Todos os pacotes com dependências não atendidas após o upgrade serão desinstalados.

7.1.4 Upgrade de distribuição com o zypper

Com o utilitário de linha de comando `zypper`, é possível fazer upgrade para a próxima versão da distribuição. O mais importante, é possível iniciar o processo de upgrade do sistema no próprio sistema que está em execução.

Esse recurso é ótimo para usuários avançados que querem executar upgrades remotos ou upgrades em diversos sistemas configurados de forma parecida.

7.1.4.1 Antes de iniciar o upgrade com o zypper

Para evitar erros inesperados durante o processo de upgrade usando o `zypper`, minimize as configurações de risco.

- Feche todos os aplicativos e serviços desnecessários possíveis e desconecte todos os usuários regulares.
- Desabilite os repositórios de terceiros antes de iniciar o upgrade, ou reduza a prioridade desses repositórios para assegurar que os pacotes dos repositórios do sistema padrão tenham preferência. Habilite-os novamente após o upgrade e edite sua versão para corresponder ao número de versão da distribuição do sistema atualizado que está em execução.
- Registre o sistema. Se isso ainda não tiver sido feito, ele poderá ser registrado usando o módulo *Configuração do Novell Customer Center* no YaST ou usando a ferramenta de linha de comando `suse_register`. Isso adiciona as fontes de atualização ao sistema.

ATENÇÃO: Faça Upgrades da Reinicialização

O processo de upgrade deve ser feito por completo, do início até a reinicialização. Existe apenas uma chance limitada de reverter as mudanças. Além disso, o servidor deve estar conectado online durante todo o processo.

7.1.4.2 Procedimento de upgrade

ATENÇÃO: Verificar backup do sistema

Antes de começar realmente o procedimento de upgrade, verifique se o backup do sistema está atualizado e pode ser restaurado. Isso é importante principalmente porque você deve inserir muitas das etapas a seguir manualmente.

O programa `zypper` suporta nomes de comandos longos e curtos. Por exemplo, é possível abreviar `zypper install` para `zypper in`. No texto a seguir, são usadas as variantes curtas.

Efetue login como `root` e siga as etapas abaixo:

1 Atualize todos os serviços e repositórios:

```
zypper ref -s
```

2 Instale as atualizações de gerenciamento de pacote:

```
zypper up -t patch
```

Para obter mais informações, consulte o Capítulo 1, *Atualização Online do YaST* (p 3).

3 Repita o Passo 2 (p 79) para instalar todas as atualizações disponíveis para o seu sistema.

Nota: Para usar o comando acima em um script para upgrade autônomo, use o comando:

```
zypper --non-interactive patch --auto-agree-with-licenses --with-interactive
```

4 Leia as informações de migração do produto em `/etc/products.d/*.prod`. Os produtos instalados incluem informações sobre upgrades de distribuição e quais produtos de migração devem ser instalados para executar a migração. Instale-os com os seguintes comandos:

4a Extraia as informações sobre o produto:

```
zypper se -t product | grep -h -- "-migration" | cut -d\| -f2
```

Veja a seguir um exemplo de saída:

```
SUSE_SLES-SP3-migration
sle-sdk-SP3-migration
```

4b Instale estes produtos de migração (exemplo):

```
zypper in -t product sle-sdk-SP3-migration SUSE_SLES-SP3-migration
```

4c Registre os produtos para obter os repositórios de atualização correspondentes:

```
suse_register -d 2 -L /root/.suse_register.log
```

ATENÇÃO: Habilite repositório adicional para usuários do SLED

Alguns pacotes de desenvolvimento (devel) foram movidos da mídia de instalação `SLED11-SP2` para o repositório `SLED11-Extras`. Para evitar conflitos de dependência durante o upgrade, habilite esse repositório antes de fazer o upgrade real. Execute `yast2 repositories` e habilite `SLED11-Extras`. No SLES, essa etapa extra não é necessária.

5 Atualize serviços e repositórios:

```
zypper ref -s
```

6 Verifique os repositórios usando o comando `zypper lr`. Se necessário, desabilite os repositórios `Pool/Core/Updates` do SP1/SP2 manualmente e habilite os novos repositórios (`SP3-Pool`, `SP3-Updates`) do SP3:

```
zypper mr --disable REPOALIAS
zypper mr --enable REPOALIAS
```

7 Faça um upgrade de distribuição usando o seguinte comando (exemplo para SLES, ajustar nomes de catálogo em caso de atualização do SLED):

```
zypper dup --from SLES11-SP3-Pool --from SLES11-SP3-Updates
```

Se necessário, você poderá adicionar mais catálogos. Por exemplo, quando produtos complementares são instalados. O Zypper avisa que vai apagar o produto de migração e atualizar os produtos principais. Confirme a mensagem para continuar atualizando os pacotes rpm.

8 Após o término do upgrade, registre os novos produtos novamente:

```
suse_register -d 2 -L /root/.suse_register.log
```

9 Reinicialize o sistema:

```
shutdown -r
```

7.1.5 Gerenciando repositórios com o zypper

Todos os comandos de instalação ou patch do zipper dependem de uma lista de repositórios conhecidos. Para listar todos os repositórios conhecidos para o sistema, use o comando:

```
zypper repos
```

O resultado parecerá com o seguinte:

Exemplo 7.1 *Zypper: lista de repositórios conhecidos*

```
# | Alias                              | Name
   | Enabled | Refresh
--+------------------------------------+------------------------------------+---------+--------
1 | SUSE-Linux-Enterprise-Server 11-0 | SUSE-Linux-Enterprise-Server 11-0
 | Yes     | No
2 | SLES-11-Updates                    | SLES 11 Online Updates
   | Yes     | Yes
3 | broadcomdrv                        | Broadcom Drivers
   | Yes     | No
```

Na especificação de repositórios em vários comandos, é possível usar um álias, URI ou número de repositório a partir da saída do comando `zypper repos`. O álias do repositório é uma versão abreviada do nome do repositório para uso em comandos de gerenciamento de repositórios. Observe que os números dos repositórios podem ser mudados após modificar a lista de repositórios. O álias nunca mudará sozinho.

Por padrão; detalhes, como o URI ou a prioridade do repositório, não são exibidos. Use o seguinte comando para listar todos os detalhes:

```
zypper repos -d
```

Às vezes, a lista inclui um grande número de repositórios que não estão habilitados, o que pode ser confuso. Para mostrar apenas os repositórios habilitados, use o seguinte comando:

```
zypper repos -E
```

7.1.5.1 Adicionando repositórios

ATENÇÃO: Possível comprometimento do sistema ao adicionar repositórios com o Zypper

Por padrão, as sínteses e assinaturas de pacotes dos repositórios fornecidos pela SUSE são verificadas para garantir sua origem e qualidade. A “Verificação GPG” está habilitada no arquivo de configuração de repositório no servidor que fornece o repositório.

Ao adicionar um repositório com o comando `zypper ar`, o download desse arquivo de configuração é feito em `/etc/zypp/repos.d`. O Zypper também informa o usuário sobre a opção Verificação GPG:

```
GPG check: Yes
```

Verifique sempre se a saída da verificação GPG está definida como “Sim”. Se estiver definida como “Não”, o sistema poderá estar comprometido por downgrades de pacotes que introduzem novamente vulnerabilidades já corrigidas, por exemplo. Não é recomendado confiar em repositórios que tenham essa opção definida como “Não”. Caso você saiba que a verificação GPG foi desabilitada por engano, habilite a opção novamente adicionando a seguinte linha ao respectivo arquivo de configuração de repositório em `/etc/zypp/repos.d`:

```
gpgcheck=1
```

Para adicionar um repositório, execute

```
zypper addrepo URIalias
```

O *`URI`* pode ser um repositório da Internet, um recurso de rede, um diretório ou um CD ou DVD (consulte http://en.opensuse.org/openSUSE:Libzypp_URIs para obter os detalhes). O *`álias`* é um identificador abreviado e exclusivo do

repositório. Pode ser escolhido livremente, com a única condição de que seja exclusivo. O zypper emitirá um aviso se você especificar um álias que já está em uso.

7.1.5.2 Removendo repositórios

Se você deseja remover um repositório da lista, use o comando `zypper removerepo` junto com o álias ou o número do repositório que você deseja apagar. Por exemplo, para remover o repositório listado como a terceira entrada no Exemplo 7.1, "Zypper: lista de repositórios conhecidos" (p 81), use o seguinte comando:

```
zypper removerepo 3
```

7.1.5.3 Modificando repositórios

Habilite ou desabilite os repositórios com `zypper modifyrepo`. Você também pode alterar as propriedades do repositório (por exemplo, atualizar o comportamento, o nome ou a prioridade) com esse comando. O comando a seguir habilita o repositório chamado `updates`, ativa a atualização automática e define sua prioridade como 20:

```
zypper modifyrepo -er -p 20 'updates'
```

A modificação de repositórios não se limita a um único repositório, você também pode operar em grupos:

`-a`: todos os repositórios
`-l`: repositórios locais
`-t`: repositórios remotos
`-m` *`TIPO`*: repositórios de um tipo específico (em que *`TIPO`* pode ser um dos seguintes: `http`, `https`, `ftp`, `cd`, `dvd`, `dir`, `file`, `cifs`, `smb`, `nfs`, `hd`, `iso`)

Para renomear o álias de um repositório, use o comando `renamerepo`. O exemplo a seguir muda o álias `Mozilla Firefox` para somente `firefox`:

```
zypper renamerepo 'Mozilla Firefox' firefox
```

7.1.6 Consultando repositórios e pacotes com o zypper

O zypper oferece vários métodos de consulta a repositórios ou pacotes. Para obter as listas de todos os produtos, padrões, pacotes ou patches disponíveis, use os seguintes comandos:

```
zypper products
zypper patterns
zypper packages
zypper patches
```

Para consultar todos os repositórios para determinados pacotes, use `search`. Ela funciona em nomes de pacotes ou, opcionalmente, em resumos e descrições de pacotes. Usando os curingas `*` e `?`com o termo da pesquisa é permitido. Por padrão, a pesquisa não diferencia maiúsculas de minúsculas.

```
zypper search firefox       # simple search for "firefox"
zypper search "*fire*"      # using wild cards
zypper search -d fire      # also search in package descriptions and summaries
zypper search -u firefox    # only display packages not already installed
```

Para procurar pacotes que oferecem um recurso específico, use o comando `what-provides`. Por exemplo, para saber qual pacote fornece o módulo perl `SVN::Core`, use o seguinte comando:

```
zypper what-provides 'perl(SVN::Core)'
```

Para consultar pacotes únicos, use `info` com um nome exato de pacote como argumento. Ele exibe informações detalhadas sobre um pacote. Para mostrar também o que é exigido/recomendado pelo pacote, use as opções `--requires` e `--recommends`:

```
zypper info --requires MozillaFirefox
```

O `what-provides` *`pacote`* é semelhante a `rpm -q --whatprovides` *`pacote`*, mas o RPM só pode consultar o banco de dados RPM (que é o banco de dados de todos os pacotes instalados). O zypper, por outro lado, o informará sobre fornecedores do recurso a partir de qualquer repositório, não apenas aqueles que estão instalados.

7.1.7 Configurando o Zypper

O Zypper agora vem com um arquivo de configuração que permite mudar permanentemente o comportamento do Zypper (de todo o sistema ou de um usuário específico). Para mudanças de todo o sistema, edite `/etc/zypp/zypper.conf`. Para mudanças específicas do usuário, edite `~/.zypper.conf`. Se `~/.zypper.conf` ainda não existir, use `/etc/zypp/zypper.conf` como modelo: copie-o para `~/.zypper.conf` e ajuste-o como preferir. Consulte os comentários no arquivo para obter ajuda sobre as opções disponíveis.

7.1.8 Solucionando problemas

Caso tenha problemas para acessar os pacotes dos repositórios configurados (por exemplo, o Zypper não encontra determinado pacote apesar de você saber que ele existe em um dos repositórios), poderá ajudar se você atualizar os repositórios com:

```
zypper refresh
```

Se isso não ajudar, tente

```
zypper refresh -fdb
```

Isso força uma atualização completa e a reconstrução do banco de dados, incluindo um download forçado dos metadados iniciais.

7.1.9 Recurso de rollback do Zypper no sistema de arquivos btrfs

Se o sistema de arquivos btrfs for usado na partição raiz e o `snapper` estiver instalado, o Zypper chamará automaticamente o `snapper` (usando o script instalado pelo `snapper`) ao confirmar as mudanças no sistema de arquivos para criar os instantâneos apropriados do sistema de arquivos. É possível usar esses instantâneos para reverter as mudanças feitas pelo zypper. Para obter mais informações sobre o `snapper`, consulte `man snapper`.

Atualmente, o Zypper (e o YaST) só cria instantâneos do sistema de arquivos raiz. Outros subvolumes não podem ser configurados. Esse recurso não é suportado no sistema de arquivos padrão.

7.2 RPM — o gerenciador de pacotes

O RPM (gerenciador de pacotes RPM) é usado para gerenciar pacotes de software. Seus principais comandos são `rpm` e `rpmbuild`. O banco de dados RPM avançado pode ser consultado pelos usuários, administradores de sistema e construtores de pacotes para obtenção de informações detalhadas sobre o software instalado.

Basicamente, o `rpm` possui cinco modos: instalação, desinstalação (ou atualização) de pacotes de software, reconstrução do banco de dados RPM, consulta de bancos RPM ou arquivos RPM individuais, verificação de integridade dos pacotes e assinatura de pacotes. O `rpmbuild` pode ser usado para construir pacotes instaláveis de fontes originais.

Os arquivos RPM instaláveis são compactados em um formato binário especial. Esses são arquivos de programa para instalação e determinadas metainformações usadas durante a instalação pelo comando `rpm` para configurar o pacote de softwares. Também são armazenados no banco de dados RPM com o objetivo de documentação. Os arquivos RPM normalmente têm a extensão `.rpm`.

DICA: pacotes de desenvolvimento de software

Para vários pacotes, os componentes necessários para o desenvolvimento de software (bibliotecas, cabeçalhos, arquivos de inclusão etc.) foram colocados em pacotes separados. Esses pacotes de desenvolvimento só são necessários quando você deseja compilar software por conta própria (por exemplo, os pacotes do GNOME mais recentes). É possível identificá-los pela extensão do nome `-devel`, como os pacotes `alsa-devel`, `gimp-devel` e `libkde4-devel`.

7.2.1 Verificando a autenticidade do pacote

Os pacotes RPM têm uma assinatura GPG. Para verificar a assinatura de um pacote RPM, use o comando `rpm --checksig` *`pacote`*`-1.2.3.rpm` para determinar se o pacote vem da Novell/SUSE ou de outra empresa confiável. Isso é especialmente recomendado para pacotes de atualização da Internet.

7.2.2 Gerenciando pacotes: instalar, atualizar e desinstalar

Normalmente, a instalação de um arquivo RPM é bem simples: `rpm -i` *`pacote`*`.rpm`. Com esse comando, o pacote é instalado, mas apenas quando suas dependências são atendidas e quando não há conflitos com outros pacotes. Com uma mensagem de erro, o `rpm` solicita os pacotes que devem ser instalados para atender a requisitos de dependência. No segundo plano, o banco de dados RPM garante que não haja conflitos, pois um arquivo específico pode pertencer somente a um pacote. Ao escolher opções diferentes, você pode forçar o `rpm` a ignorar esses padrões, mas isso é somente para especialistas. Caso contrário, você se arrisca a comprometer a integridade do sistema e, possivelmente, ameaça a capacidade de atualização do sistema.

As opções `-U` ou `--upgrade` e `-F` ou `--freshen` podem ser usadas para atualizar um pacote (por exemplo, `rpm -F` *`pacote`*`.rpm`). Esse comando remove os arquivos da versão antiga e instala os novos arquivos imediatamente. A diferença entre as duas versões é que o `-U` instala pacotes que não existiam no sistema anteriormente, mas `-F` atualiza somente pacotes previamente instalados. Durante a atualização, o `rpm` atualiza arquivos de configuração cuidadosamente com a seguinte estratégia:

- Se um arquivo de configuração não tiver sido modificado pelo administrador de sistema, o `rpm` instalará a nova versão do arquivo apropriado. O administrador de sistema não precisa adotar nenhuma ação.

- Se um arquivo de configuração tiver sido mudado pelo administrador do sistema antes da atualização, o `rpm` gravará o arquivo mudado com a extensão `.rpmorig` ou `.rpmsave` (arquivo de backup) e instalará a versão do novo pacote (mas somente se o arquivo instalado originalmente e a versão mais nova forem diferentes). Nesse caso, compare o arquivo de backup (`.rpmorig` ou `.rpmsave`) com o arquivo recém-instalado e faça novamente as modificações no novo arquivo. Depois, verifique se apagou todos os arquivos `.rpmorig` e `.rpmsave` para evitar problemas em atualizações futuras.

- Arquivos `.rpmnew` são exibidos se o arquivo de configuração já existir *e* se o rótulo `noreplace` tiver sido especificado no arquivo `.spec`.

Após uma atualização, os arquivos `.rpmsave` e `.rpmnew` devem ser removidos depois de comparados, para que não impeçam atualizações futuras. A extensão

.rpmorig será atribuída se o arquivo não tiver sido previamente reconhecido pelo banco de dados RPM.

Caso contrário, o .rpmsave será usado. Em outras palavras, o .rpmorig resulta da atualização de um formato estranho ao RPM. O .rpmsave resulta da atualização de um RPM mais antigo para um RPM mais novo. O .rpmnew não revela se o administrador do sistema fez mudanças no arquivo de configuração. Uma lista destes arquivos está disponível em /var/adm/rpmconfigcheck. Alguns arquivos de configuração (como /etc/httpd/httpd.conf) não são sobregravados para permitir operação continuada.

O switch -U *não* é somente um equivalente para a desinstalação com a opção -e e a instalação com a opção -i. Use -U sempre que possível.

Para remover um pacote, digite rpm -e *pacote*. O rpm, que só apaga o pacote quando não há dependências não resolvidas. É teoricamente impossível apagar Tcl/Tk, por exemplo, enquanto outro aplicativo exigir sua existência. Mesmo nesse caso, o RPM pede ajuda do banco de dados. Se, por qualquer motivo, a exclusão for impossível (mesmo que não exista *nenhuma* dependência adicional), talvez seja útil reconstruir o banco de dados RPM usando a opção --rebuilddb.

7.2.3 RPM e patches

Para garantir a segurança operacional de um sistema, pacotes de atualização devem ser instalados no sistema periodicamente. Anteriormente, um erro em um pacote só poderia ser eliminado com a substituição de todo o pacote. Pacotes grandes com bugs em pequenos arquivos podem resultar facilmente nesse cenário. Porém, o RPM do SUSE oferece um recurso que permite a instalação de patches em pacotes.

Como exemplo, as considerações mais importantes são demonstradas com pine:

O RPM com patch é adequado para meu sistema?
: Para verificar isso, consulte primeiro a versão instalada do pacote. No caso do pine, isso pode ser feito com

```
rpm -q pine
pine-4.44-188
```

Em seguida, verifique se o RPM com patch é adequado para essa versão do pine:

```
rpm -qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

Esse patch é adequado para três versões diferentes do pine. A versão instalada no exemplo também está listada para que o patch possa ser instalado.

Quais arquivos serão substituídos pelo patch?

Os arquivos afetados por um patch podem ser facilmente vistos no RPM com patch. O parâmetro `rpm-P permite a seleção de recursos de patch especiais.` Exiba a lista de arquivos com o seguinte comando:

```
rpm -qpPl pine-4.44-224.i586.patch.rpm
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

ou, se o patch já estiver instalado, com o seguinte comando:

```
rpm -qPl pine
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

Como instalar um RPM com patch no sistema?

RPMs com patch são usados como RPMs comuns. A única diferença é que um RPM adequado já deve estar instalado.

Quais patches já estão instalados no sistema e para quais versões do pacote?

É possível exibir uma lista de todos os patches instalados no sistema com o comando `rpm -qPa`. Se somente um patch for instalado em um novo sistema (como no exemplo), a lista será exibida como a seguir:

```
rpm -qPa
pine-4.44-224
```

Se posteriormente você desejar saber qual versão de pacote foi originalmente instalada, essas informações também estarão disponíveis no banco de dados RPM. No caso do `pine`, é possível exibir essas informações com o seguinte comando:

```
rpm -q --basedon pine
pine = 4.44-188
```

Mais informações, incluindo informações sobre o recurso de patch do RPM, estão disponíveis nas páginas de manual de `rpm` e `rpmbuild`.

NOTA: Atualizações oficiais para o SUSE Linux Enterprise Desktop

Para que o tamanho do download das atualizações seja o menor possível, as atualizações oficiais para o SUSE Linux Enterprise Desktop não são fornecidas como RPMs de Patch, mas sim como pacotes RPM Delta. Para obter os detalhes, consulte a Seção 7.2.4, “Pacotes RPM Delta” (p 90).

7.2.4 Pacotes RPM Delta

Os pacotes RPM Delta possuem uma diferença entre uma versão nova e antiga de um pacote RPM. Aplicar um RPM delta a um RPM antigo resulta em um RPM completamente novo. Não é necessário ter uma cópia do RPM antigo, pois um RPM delta também pode funcionar com um RPM instalado. Os pacotes RPM delta têm tamanho ainda menor que os RPMs com patch, o que é uma vantagem durante a transferência de pacotes de atualização na Internet. A desvantagem é que operações de atualização que envolvem RPMs delta consomem consideravelmente mais ciclos de CPU do que as operações com RPMs com patch ou simples.

Os binários `prepdeltarpm`, `writedeltarpm` e `applydeltarpm` integram a suíte de RPM delta (pacote `deltarpm`) e ajudam na criação e aplicação de pacotes RPM delta. Com os seguintes comandos, crie um RPM delta chamado `new.delta.rpm`. O comando a seguir pressupõe que `old.rpm` e `new.rpm` estejam presentes:

```
prepdeltarpm -s seq -i info old.rpm > old.cpio
prepdeltarpm -f new.rpm > new.cpio
xdelta delta -0 old.cpio new.cpio delta
writedeltarpm new.rpm delta info new.delta.rpm
```

Por fim, remova os arquivos de trabalho temporários `old.cpio`, `new.cpio` e `delta`.

Usando `applydeltarpm`, você poderá reconstruir o novo RPM do arquivo de sistema, se o pacote antigo já estiver instalado:

```
applydeltarpm new.delta.rpm new.rpm
```

Para derivá-lo do RPM antigo sem acessar o sistema de arquivos, use a opção `-r`:

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

Consulte `/usr/share/doc/packages/deltarpm/README` para obter os detalhes técnicos.

7.2.5 Consultas de RPM

Com a opção -q, o rpm inicia consultas, permitindo a inspeção de um arquivo RPM (adicionando-se a opção -p) e também a consulta ao banco de dados RPM de pacotes instalados. Vários switches estão disponíveis para especificar o tipo de informação necessária. Consulte a Tabela 7.1, “Opções mais importantes de consulta de RPM” (p 91).

***Tabela 7.1** Opções mais importantes de consulta de RPM*

-i	Informações de pacote
-l	Lista de arquivos
-f ARQUIVO	Consulte o pacote que contém o arquivo *ARQUIVO* (o caminho completo deve ser especificado com *ARQUIVO*)
-s	Lista de arquivos com informações de status (requer -l)
-d	Lista somente arquivos de documentação (requer -l)
-c	Lista somente arquivos de configuração (requer -l)
--dump	Lista de arquivos com detalhes completos (a ser usada com -l, -c ou -d)
--provides	Lista recursos do pacote que outro pacote pode solicitar com --requires
--requires, -R	Recursos exigidos pelo pacote

`--scripts`	Scripts de instalação (pré-instalação, pós-instalação, desinstalação)

Por exemplo, o comando `rpm -q -i wget` exibe as informações mostradas no Exemplo 7.2, "rpm -q -i wget" (p 92).

***Exemplo 7.2** rpm -q -i wget*

```
Name        : wget                          Relocations: (not relocatable)
Version     : 1.11.4                             Vendor: openSUSE
Release     : 1.70                           Build Date: Sat 01 Aug 2009
09:49:48 CEST
Install Date: Thu 06 Aug 2009 14:53:24 CEST      Build Host: build18
Group       : Productivity/Networking/Web/Utilities   Source RPM:
wget-1.11.4-1.70.src.rpm
Size        : 1525431                          License: GPL v3 or later
Signature   : RSA/8, Sat 01 Aug 2009 09:50:04 CEST, Key ID b88b2fd43dbdc284
Packager    : http://bugs.opensuse.org
URL         : http://www.gnu.org/software/wget/
Summary     : A Tool for Mirroring FTP and HTTP Servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

A opção `-f` funciona somente se você especificar o nome e o caminho completos do arquivo. Forneça quantos nomes de arquivo desejar. Por exemplo, o seguinte comando

```
rpm -q -f /bin/rpm /usr/bin/wget
```

resulta em:

```
rpm-4.8.0-4.3.x86_64
wget-1.11.4-11.18.x86_64
```

Se somente parte do nome de arquivo for conhecida, use um script de shell conforme mostrado no Exemplo 7.3, "Script para pesquisar pacotes" (p 92). Passe o nome de arquivo parcial para o script mostrado como um parâmetro ao executá-lo.

***Exemplo 7.3** Script para pesquisar pacotes*

```
#! /bin/sh
for i in $(rpm -q -a -l | grep $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
    echo ""
done
```

O comando `rpm -q --changelog rpm` exibe uma lista detalhada com as informações de modificações sobre determinado pacote (neste caso, o pacote `rpm`), classificadas por data.

Com a ajuda do banco de dados RPM instalado, é possível realizar verificações. Inicie as verificações com `-V`, `-y` ou `--verify`. Com essa opção, o `rpm` mostra todos os arquivos em um pacote que foram modificados desde a instalação. O `rpm` usa oito símbolos de caracteres para fornecer algumas dicas sobre as seguintes mudanças:

***Tabela 7.2** Opções de verificação do RPM*

`5`	Resumo de verificação MD5
`S`	Tamanho do arquivo
`L`	Link simbólico
`T`	Tempo de modificação
`D`	Números de dispositivo principais e auxiliares
`U`	Proprietário
`G`	Grupo
`M`	Modo (tipo de arquivo e permissões)

No caso de arquivos de configuração, a letra `c` é impressa. Por exemplo, para modificações no pacote `/etc/wgetrc` (`wget`):

```
rpm -V wget
S.5....T c /etc/wgetrc
```

Os arquivos do banco de dados RPM são colocados em `/var/lib/rpm`. Se a partição `/usr` tiver o tamanho de 1 GB, esse banco de dados poderá ocupar praticamente 30 MB, especialmente após uma atualização completa. Se o banco de dados for maior do que o esperado, será útil reconstruir o banco de dados com a opção `--rebuilddb`. Antes disso, faça um backup do banco de dados antigo. O script `cron` `cron.daily` faz cópias diárias do banco de dados (compactado com gzip) e as armazena em `/var/`

adm/backup/rpmdb. O número de cópias é controlado pela variável MAX_RPMDB_BACKUPS (padrão: 5) em /etc/sysconfig/backup. O tamanho de um único backup é de aproximadamente 1 MB para 1 GB em /usr.

7.2.6 Instalando e compilando pacotes de fonte

Todos os pacotes de fonte têm a extensão .src.rpm (RPM de fonte).

NOTA: Pacotes de fontes instalados

Pacotes de fonte podem ser copiados da mídia de instalação para o disco rígido e descompactados com o YaST. Porém, eles não são marcados como instalados ([i]) no gerenciador de pacotes. Isso ocorre porque os pacotes de fontes não são inseridos no banco de dados RPM. Somente o software do sistema operacional *instalado* está listado no banco de dados RPM. Quando você "instalar" um pacote de fontes, somente o código-fonte será adicionado ao sistema.

Os diretórios a seguir devem estar disponíveis para rpm e rpmbuild em /usr/src/packages (a menos que você tenha especificado configurações personalizadas em um arquivo como /etc/rpmrc):

SOURCES
: para as fontes originais (arquivos .tar.bz2 ou .tar.gz etc.) e para ajustes específicos de distribuição (geralmente arquivos .diff ou .patch)

SPECS
: para os arquivos .spec, similares a um metaMakefile, que controla o processo de *construção*

BUILD
: diretório em que todas as fontes são descompactadas, corrigidas e compiladas

RPMS
: local em que os pacotes binários concluídos são armazenados

SRPMS
: local em que estão os RPMs de fonte

Quando você instala um pacote de fontes com o YaST, todos os componentes necessários são instalados em /usr/src/packages: as fontes e os ajustes em SOURCES e o arquivo .spec relevante em SPECS.

ATENÇÃO

Não faça experiências com os componentes do sistema (glibc, rpm, sysvinit etc.), pois isso arrisca a estabilidade do sistema.

O exemplo a seguir usa o pacote wget.src.rpm. Após instalar o pacote de origem, você deverá ter arquivos semelhantes aos da seguinte lista:

```
/usr/src/packages/SOURCES/wget-1.11.4.tar.bz2
/usr/src/packages/SOURCES/wgetrc.patch
/usr/src/packages/SPECS/wget.spec
```

rpmbuild -b *X* /usr/src/packages/SPECS/wget.spec inicia a compilação. *X* é um curinga para vários estágios do processo de construção (consulte a saída de --help ou a documentação do RPM para obter os detalhes). Veja a seguir uma breve explicação:

-bp
: Preparar as fontes em /usr/src/packages/BUILD: descompactar e corrigir.

-bc
: Faz o mesmo que -bp, mas com compilação adicional.

-bi
: Faz o mesmo que -bp, mas com a instalação adicional do software criado. Cuidado: se o pacote não aceitar o recurso BuildRoot, talvez você sobregrave os arquivos de configuração.

-bb
: Faz o mesmo que -bi, mas com a criação adicional do pacote binário. Se a compilação tiver sido bem-sucedida, o binário deverá estar em /usr/src/packages/RPMS.

`-ba`
: Faz o mesmo que `-bb`, mas com a criação adicional do RPM de fonte. Se a compilação tiver sido bem-sucedida, o binário deverá estar em `/usr/src/packages/SRPMS`.

`--short-circuit`
: Ignora algumas etapas.

O RPM binário criado agora pode ser instalado com `rpm -i` ou, de preferência, com `rpm -U`. A instalação com `rpm` faz com que ele apareça no banco de dados RPM.

7.2.7 Compilando pacotes RPM com build

O perigo de vários pacotes é que arquivos indesejados são adicionados ao sistema em execução durante o processo de construção. Para evitar isso, use `build`, que cria um ambiente definido para construção do pacote. Para estabelecer esse ambiente chroot, o script `build` deve ser fornecido com uma árvore de pacote completa. Essa árvore pode ser disponibilizada no disco rígido, por meio do NFS ou DVD. Defina a posição com `build --rpms` *`diretório`*. Diferentemente do `rpm`, o comando `build` procura o arquivo `.spec` no diretório de fontes. Para construir o `wget` (como no exemplo acima) com o DVD montado no sistema em `/media/dvd`, use o seguinte comando como `root`:

```
cd /usr/src/packages/SOURCES/
mv ../SPECS/wget.spec .
build --rpms /media/dvd/suse/ wget.spec
```

Depois disso, um ambiente mínimo é estabelecido em `/var/tmp/build-root`. O pacote é criado nesse ambiente. Após a conclusão, os pacotes resultantes estarão localizados em `/var/tmp/build-root/usr/src/packages/RPMS`.

O script `build` oferece várias opções adicionais. Por exemplo, fazer com que o script prefira seus próprios RPMs, omitir a inicialização do ambiente de construção ou limitar o comando `rpm` a um dos estágios mencionados acima. Acesse informações adicionais com `build --help` e a leitura da página de manual `build`.

7.2.8 Ferramentas para arquivos RPM e banco de dados RPM

O Midnight Commander (mc) pode exibir o conteúdo de arquivos RPM e copiar partes deles. Ele representa arquivos como sistemas de arquivos virtuais, oferecendo todas as opções de menu usuais do Midnight Commander. Exiba o HEADER com F3. Exiba a estrutura de arquivos com as teclas de cursor e Enter. Copie componentes de arquivos com F5.

Um gerenciador de pacote completo está disponível como um módulo do YaST. Para obter os detalhes, consulte o Chapter 6, *Installing or Removing Software* (↑*Deployment Guide*).

8 Bash e scripts Bash

Atualmente, muitas pessoas usam computadores com uma GUI (interface gráfica de usuário) como KDE ou GNOME. Embora ela ofereça muitos recursos, seu uso é limitado quando se trata de execução de tarefas automatizadas. Shells são bons aliados das interfaces gráficas, por isso este capítulo apresenta uma visão geral de alguns aspectos dos shells, neste caso, o Bash.

8.1 O que é “o shell”?

Tradicionalmente, *o* shell é o Bash (Bourne again Shell). Quando este capítulo menciona “o shell”, ele se refere ao Bash. Na verdade, há mais shells disponíveis além do Bash (ash, csh, ksh, zsh, etc.), cada um deles empregando recursos e características diferentes. Se você precisar de mais informações sobre outros shells, pesquise por *shell* no YaST.

8.1.1 Conhecendo os arquivos de configuração do Bash

Um shell pode ser acionado como:

1. **Shell de login interativo** Esse tipo é usado para efetuar login em uma máquina, chamando o Bash com a opção `--login`, ou para efetuar login em uma máquina remota com SSH.

2. **Shell interativo “comum”** Normalmente esse é o caso quando se inicia o xterm, o konsole, o gnome-terminal ou ferramentas semelhantes.

3. **Shell não interativo** Usado para chamar um script de shell na linha de comando.

Dependendo do tipo de shell usado, variam os arquivos de configuração lidos. As tabelas seguintes mostram os arquivos de configuração de shell de login e sem login.

***Tabela 8.1** Arquivos de configuração do Bash para shells de login*

Arquivo	Descrição
`/etc/profile`	Não modifique esse arquivo, senão as suas modificações poderão ser destruídas durante a próxima atualização!
`/etc/profile.local`	Use esse arquivos se for estender `/etc/profile`
`/etc/profile.d/`	Contém arquivos de configuração de programas específicos para todo o sistema
`~/.profile`	Insira aqui a configuração específica de usuário para os shells de login

***Tabela 8.2** Arquivos de configuração do Bash para shells sem login*

`/etc/bash.bashrc`	Não modifique esse arquivo, senão as suas modificações poderão ser destruídas durante a próxima atualização!
`/etc/bash.bashrc.local`	Use esse arquivo para inserir suas modificações apenas do Bash em todo o sistema
`~/.bashrc`	Insira aqui a configuração específica de usuário

Além desses, o Bash usa mais outros arquivos:

Tabela 8.3 *Arquivos especiais do Bash*

Arquivo	Descrição
~/.bash_history	Contém uma lista de todos os comandos que você digitou
~/.bash_logout	Executado durante o logout

8.1.2 Estrutura de diretórios

A tabela a seguir fornece uma breve visão geral dos mais importantes diretórios de nível superior encontrados em um sistema Linux. Informações mais detalhadas sobre os diretórios e subdiretórios importantes são encontradas na lista a seguir.

Tabela 8.4 *Visão geral de uma árvore de diretório padrão*

Diretório	Conteúdo
/	Diretório raiz: o ponto de partida da árvore do diretório.
/bin	Arquivos binários essenciais, como comandos necessários pelo administrador do sistema e por usuários comuns. Geralmente contém os shells, como o Bash.
/boot	Arquivos estáticos do carregador de boot.
/dev	Arquivos necessários para acessar dispositivos específicos de host.
/etc	Arquivos de configuração do sistema específicos de host.

Diretório	Conteúdo
`/home`	Contém os diretórios pessoais de todos os usuários que possuem conta no sistema. Porém, o diretório pessoal do `root` não está em `/home`, mas sim em `/root`.
`/lib`	Bibliotecas compartilhadas e módulos de kernel essenciais.
`/media`	Pontos de montagem de mídia removível.
`/mnt`	Ponto de montagem para montar temporariamente um sistema de arquivos.
`/opt`	Pacotes de aplicativos complementares.
`/root`	Diretório pessoal do superusuário `root`.
`/sbin`	Binários essenciais do sistema.
`/srv`	Dados de serviços fornecidos pelo sistema.
`/tmp`	Arquivos temporários.
`/usr`	Hierarquia secundária com dados apenas leitura.
`/var`	Dados variáveis, como arquivos de registro.
`/windows`	Disponível apenas se você tiver o Microsoft Windows* e o Linux

Diretório	Conteúdo
	instalados no sistema. Contém os dados do Windows.

A lista a seguir fornece informações mais detalhadas e alguns exemplos de arquivos e subdiretórios encontrados nos diretórios:

`/bin`
: Contém comandos básicos do shell que podem ser usados pelo `root` e por outros usuários. Esses comandos incluem `ls`, `mkdir`, `cp`, `mv`, `rm` e `rmdir`. O `/bin` também contém o Bash, o shell padrão do SUSE Linux Enterprise Desktop.

`/boot`
: Contém dados necessários para inicializar, como o carregador de boot, o kernel e outros dados usados para que o kernel possa executar programas em modo de usuário.

`/dev`
: Contém arquivos de dispositivos que representam componentes de hardware.

`/etc`
: Contém arquivos de configuração local que controlam a operação de programas como o Sistema X Window. O subdiretório `/etc/init.d` contém scripts que são executados durante o processo de boot.

`/home/`*`nome_do_usuário`*
: Contém os dados privados de todos os usuários que possuem uma conta no sistema. Os arquivos localizados aqui apenas podem ser modificados por seu proprietário ou pelo administrador do sistema. Por padrão, seu diretório de e-mail e sua configuração de área de trabalho pessoal estão localizados aqui, na forma de arquivos e diretórios ocultos. Usuários do KDE encontram os dados de configuração pessoal da área de trabalho em `.kde4`; os usuários do GNOME os encontram em `.gconf`.

NOTA: diretório pessoal em um ambiente de rede

Se você estiver trabalhando em um ambiente de rede, seu diretório pessoal poderá ser mapeado para um diretório no sistema de arquivos diferente de `/home`.

`/lib`
: Contém as bibliotecas compartilhadas essenciais necessárias para inicializar o sistema e executar os comandos no sistema de arquivos raiz. O equivalente no Windows para as bibliotecas compartilhadas são os arquivos DLL.

`/media`
: Contém pontos de montagem para mídia removível, como CD-ROMs, cartões USB e câmeras digitais (se usarem USB). `/media` geralmente mantém qualquer tipo de unidade, exceto o disco rígido do seu sistema. Assim que a mídia removível for inserida ou conectada no sistema e estiver montada, você poderá acessá-la a partir daqui.

`/mnt`
: O diretório fornece um ponto de montagem para um sistema de arquivos montado temporariamente. O `root` pode montar sistemas de arquivos aqui.

`/opt`
: Reservado para a instalação de software de terceiros. Software opcional e pacotes de programas complementares maiores são encontrados aqui.

`/root`
: Diretório pessoal do usuário `root`. Os dados pessoais do `root` estão localizados aqui.

`/sbin`
: Como indicado pelo `s`, esse diretório contém utilitários do superusuário. `/sbin` contém os binários essenciais para boot, restauração e recuperação do sistema, além dos binários em `/bin`.

`/srv`
: Contém dados de serviços fornecidos pelo sistema, como FTP e HTTP.

/tmp
: Esse diretório é usado por programas que exigem o armazenamento temporário dos arquivos.

IMPORTANTE: Limpando `/tmp` em tempo de boot

Os dados armazenados em /tmp podem não existir após uma reinicialização do sistema. Depende, por exemplo, das configurações em /etc/sysconfig/cron.

/usr
: /usr não tem relação com os usuários, trata-se de um acrônimo de recursos de sistema do UNIX. Os dados em /usr são estáticos e apenas leitura, podendo ser compartilhados entre vários hosts em conformidade com o FHS (Filesystem Hierarchy Standard — Padrão da Hierarquia do Sistema de Arquivos). Esse diretório contém todos os programas aplicativos e estabelece uma segunda hierarquia no sistema de arquivos. O KDE4 e o GNOME também estão localizados aqui. /usr contém alguns subdiretórios como /usr/bin, /usr/sbin, /usr/local e /usr/share/doc.

/usr/bin
: Contém programas geralmente acessíveis.

/usr/bin
: Contém programas reservados ao administrador do sistema, como as funções de reparo.

/usr/local
: Nesse diretório, o administrador do sistema pode instalar extensões locais e independentes de distribuição.

/usr/share/doc
: Contém vários arquivos de documentação e as notas de versão do sistema. No subdiretório manual, você encontra uma versão online deste manual. Se houver mais de um idioma instalado, esse diretório poderá conter versões dos manuais em idiomas diferentes.

Em packages, você encontra a documentação incluída nos pacotes de software instalados no sistema. Para cada pacote, é criado um subdiretório /usr/share/

`doc/packages/`*`nome_do_pacote`*, geralmente contendo arquivos README do pacote e, por vezes, exemplos, arquivos de configuração ou scripts adicionais.

Se houver HOWTOs instalados no sistema, `/usr/share/doc` também conterá o subdiretório `howto`, com documentação adicional sobre muitas tarefas relacionadas a configuração e operação do software Linux.

`/var`
: Ao passo que `/usr` contém dados estáticos apenas leitura, `/var` destina-se aos dados gravados durante a operação do sistema, portanto variáveis, como arquivos de registro ou de spool. Para obter uma visão geral dos arquivos de registro mais importantes que estão em `/var/log/`, consulte a Tabela 31.1, “Arquivos de registro” (p 436).

`/windows`
: Disponível apenas se você tiver o Microsoft Windows e o Linux instalados no sistema. Contém os dados do Windows disponíveis na partição Windows do sistema. A sua capacidade de editar dados nesse diretório depende do sistema de arquivos usado pelas partições Windows. No caso do FAT32, você pode abrir e editar os arquivos desse diretório. Para NTFS, o SUSE Linux Enterprise Desktop também oferece suporte a acesso de gravação. No entanto, o driver para o sistema de arquivos NTFS-3g possui funcionalidade limitada. .

8.2 Gravando scripts shell

Scripts shell são convenientes para todos os tipos de tarefas: coleta de dados, pesquisa por uma palavra ou frase em um texto e muitas outras coisas úteis. O exemplo seguinte mostra um pequeno script shell que imprime um texto:

Exemplo 8.1 *Um script shell que imprime um texto*

```
#!/bin/sh ❶
# Output the following line: ❷
echo "Hello World" ❸
```

❶ A primeira linha começa com os caracteres *Shebang* (`#!`), indicando que o arquivo é um script. O script é executado pelo interpretador especificado após o Shebang, neste caso, `/bin/sh`.

❷ A segunda linha é um comentário que começa com o sinal de hash. Ele é recomendado para inserir comentário em linhas cuja função é difícil de lembrar.

❸ A terceira linha usa o comando interno `echo` para imprimir o texto correspondente.

Antes de executar esse script, você precisa de alguns pré-requisitos:

1. Todo script deve conter uma linha Shebang (como foi o caso do nosso exemplo acima). Se um script não tiver essa linha, você deverá chamar o interpretador manualmente.

2. Grave o script no lugar desejado. Contudo, convém gravá-lo em um diretório onde o shell possa encontrá-lo. O caminho de pesquisa em um shell é determinado pela variável de ambiente `PATH`. Um usuário normal geralmente não tem acesso de gravação em `/usr/bin`. Por essa razão, recomenda-se gravar seus scripts no diretório `~/bin/` dos usuários. O exemplo acima leva o nome `hello.sh`.

3. O script requer permissões de executável. Defina as permissões com o seguinte comando:

   ```
   chmod +x ~/bin/hello.sh
   ```

Se você atendeu a todos os pré-requisitos acima, poderá executar o script das seguintes maneiras:

1. **Como caminho absoluto** O script pode ser executado em um caminho absoluto. No nosso caso, ele é `~/bin/hello.sh`.

2. **Em todos os lugares** Se a variável de ambiente `PATH` contiver o diretório onde o script está localizado, você poderá executar o script apenas com `hello.sh`.

8.3 Redirecionando eventos de comando

Cada comando pode usar três canais, seja para entrada ou para saída:

- **Saída padrão** Esse é o canal de saída padrão. Sempre que um comando imprime algo, ele usa o canal de saída padrão.

- **Entrada padrão** Se um comando precisar da entrada dos usuários ou de outros comandos, ele usará esse canal.

- **Erro padrão** Os comandos usam esse canal para gerar relatórios de erros.

Para redirecionar os canais, as possibilidades são as seguintes:

`Comando > Arquivo`
: Grava a saída do comando em um arquivo, apagando um arquivo existente. Por exemplo, o comando `ls` grava sua saída no arquivo `listing.txt`:

```
ls > listing.txt
```

`Comando >> Arquivo`
: Anexa a saída do comando a um arquivo. Por exemplo, o comando `ls` anexa sua saída ao arquivo `listing.txt`:

```
ls >> listing.txt
```

`Comando < Arquivo`
: Lê o arquivo como entrada do comando em questão. Por exemplo, o comando `read` extrai o conteúdo do arquivo para a variável:

```
read a < foo
```

`Comando1 | Comando2`
: Redireciona a saída do comando à esquerda como entrada para o comando à direita. Por exemplo, o comando `cat` gera a saída do conteúdo do arquivo `/proc/cpuinfo`. Essa saída é usada por `grep` para filtrar apenas as linhas que contêm `cpu`:

```
cat /proc/cpuinfo | grep cpu
```

Cada canal possui um *descritor de arquivo*: 0 (zero) para entrada padrão, 1 para saída padrão e 2 para erro padrão. É permitido inserir esse descritor de arquivo antes de um caractere < ou >. Por exemplo, a linha a seguir procura por um arquivo que começa com `foo`, mas suprime seus erros redirecionando-o para `/dev/null`:

```
find / -name "foo*" 2>/dev/null
```

8.4 Usando álias

Um álias é uma definição de atalho de um ou mais comandos. A sintaxe de um álias é a seguinte:

```
alias NAME=DEFINITION
```

Por exemplo, a linha a seguir define um álias `lt` que gera uma listagem extensa (opção `-l`), classifica-a por horário de modificação (`-t`) e imprime-a em ordem inversa ao classificar (`-r`):

```
alias lt='ls -ltr'
```

Para ver todas as definições de álias, use `alias` Remova o seu álias com `unalias` e o nome de álias correspondente.

8.5 Usando variáveis no Bash

Uma variável de shell pode ser global ou local. Variáveis globais, ou de ambiente, podem ser acessadas em todos os shells. As variáveis locais, ao contrário, são visíveis apenas no shell atual.

Para ver todas as variáveis de ambiente, use o comando `printenv`. Se for preciso saber o valor de uma variável, insira o nome da variável como argumento:

```
printenv PATH
```

Uma variável, seja ela global ou local, também pode ser visualizada com `echo`:

```
echo $PATH
```

Para definir uma variável local, use um nome de variável, seguido pelo sinal de igual, seguido pelo valor:

```
PROJECT="SLED"
```

Não insira espaços antes e depois do sinal de igual, senão você obterá um erro. Para definir uma variável de ambiente, use `export`:

```
export NAME="tux"
```

Para remover uma variável, use `unset`:

```
unset NAME
```

A tabela a seguir contém algumas variáveis de ambiente comuns que podem ser usadas nos seus scripts shell:

Tabela 8.5 Variáveis de ambiente úteis

HOME	diretório pessoal do usuário atual
HOST	o nome de host atual
LANG	quando uma ferramenta é localizada, ela usa o idioma dessa variável de ambiente. Também é possível definir o idioma inglês como C
PATH	caminho de pesquisa do shell, uma lista de diretórios separados por dois-pontos
PS1	especifica o prompt normal impresso antes de cada comando
PS2	especifica o prompt secundário impresso quando você executa um comando em várias linhas
PWD	diretório de trabalho atual
USER	usuário atual

8.5.1 Usando variáveis de argumento

Por exemplo, se você tiver o script `foo.sh`, poderá executá-lo desta maneira:

```
foo.sh "Tux Penguin" 2000
```

Para acessar todos os argumentos que são passados ao seu script, você precisa de parâmetros de posição. Isto é, `$1` para o primeiro argumento, `$2` para o segundo e assim sucessivamente. É possível usar até nove parâmetros. Para obter o nome do script, use `$0`.

O script `foo.sh` a seguir imprime todos os argumentos de 1 a 4:

```
#!/bin/sh
echo \"$1\" \"$2\" \"$3\" \"$4\"
```

Se você executar esse script com os argumentos acima, obterá:

```
"Tux Penguin" "2000" "" ""
```

8.5.2 Usando substituição de variável

As substituições de variáveis aplicam um padrão ao conteúdo de uma variável, seja da esquerda ou da esquerda. A lista a seguir contém as formas de sintaxe possíveis:

`${VAR#padrão}`
: remove a correspondência mais curta possível da esquerda:

```
file=/home/tux/book/book.tar.bz2
echo ${file#*/}
home/tux/book/book.tar.bz2
```

`${VAR##padrão}`
: remove a correspondência mais longa possível da esquerda:

```
file=/home/tux/book/book.tar.bz2
echo ${file##*/}
book.tar.bz2
```

`${VAR%padrão}`
: remove a correspondência mais curta possível da direita:

```
file=/home/tux/book/book.tar.bz2
echo ${file%.*}
/home/tux/book/book.tar
```

`${VAR%%padrão}`
: remove a correspondência mais longa possível da direita:

```
file=/home/tux/book/book.tar.bz2
echo ${file%%.*}
/home/tux/book/book
```

`${VAR/padrão_1/padrão_2}`
: substitui o conteúdo de *`VAR`* do *`padrão_1`* pelo do *`padrão_2`*:

```
file=/home/tux/book/book.tar.bz2
echo ${file/tux/wilber}
/home/wilber/book/book.tar.bz2
```

8.6 Agrupando e combinando comandos

Os shells permitem concatenar e agrupar comandos para uma execução condicional. Cada comando retorna um código de saída que determina o sucesso ou a falha de sua operação. Se o código for 0 (zero), significa que o comando obteve sucesso. Todos os outros códigos significam erro específico do comando.

A lista a seguir mostra como os comandos podem ser agrupados:

`Comando1 ; Comando2`
: executa os comandos em sequência. O código de saída não é verificado. A linha a seguir exibe o conteúdo do arquivo com `cat` e depois imprime suas propriedades com `ls`, independentemente dos códigos de erro:

```
cat filelist.txt ; ls -l filelist.txt
```

`Comando1 && Comando2`
: executa o comando à direita quando o comando à esquerda for bem-sucedido (E lógico). A linha a seguir exibe o conteúdo do arquivo e imprime suas propriedades apenas quando o comando anterior obtiver sucesso (compare com a entrada anterior nesta lista):

```
cat filelist.txt && ls -l filelist.txt
```

`Comando1 || Comando2`
: executa o comando à direita quando o comando da esquerda falhar (OU lógico). A linha a seguir cria um diretório em `/home/wilber/bar` apenas quando a criação do diretório em `/home/tux/foo` falhar:

```
mkdir /home/tux/foo || mkdir /home/wilber/bar
```

`nome_da_função(){ ... }`
: cria uma função shell. Você pode usar os parâmetros de posição para acessar seus argumentos. A linha a seguir define a função `hello` para imprimir uma mensagem curta:

```
hello() { echo "Hello $1"; }
```

Você pode chamar essa função assim:

```
hello Tux
```

que imprimirá:

```
Hello Tux
```

8.7 Trabalhando com construções de fluxo comuns

Para controlar o fluxo do seu script, um shell possui as construções `while`, `if`, `for` e `case`.

8.7.1 Comando de controle if

O comando `if` é usado para verificar expressões. Por exemplo, o código a seguir testa se o usuário atual é Tux:

```
if test $USER = "tux"; then
  echo "Hello Tux."
else
  echo "You are not Tux."
fi
```

A expressão de teste pode ser tão complexa ou simples quanto possível. a expressão a seguir verifica se o arquivo `foo.txt` existe:

```
if test -e /tmp/foo.txt ;
then
  echo "Found foo.txt"
fi
```

A expressão de teste também pode ser abreviada entre colchetes:

```
if [ -e /tmp/foo.txt ] ; then
  echo "Found foo.txt"
fi
```

Outras expressões úteis estão disponíveis em `http://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/lsst/ch03sec02.html`.

8.7.2 Criando loops com o comando for

O loop `for` permite executar comandos para uma lista de entradas. Por exemplo, o código a seguir imprime algumas informações sobre arquivos PNG no diretório atual:

```
for i in *.png; do
 ls -l $i
done
```

8.8 Para obter mais informações

Informações importantes sobre o Bash são fornecidas nas páginas de manual `man bash`. Mais informações sobre este tópico estão disponíveis na lista a seguir:

- http://tldp.org/LDP/Bash-Beginners-Guide/html/index.html— Bash Guide for Beginners (Guia do Bash para Iniciantes)
- http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html— BASH Programming - Introduction HOW-TO (COMO FAZER Programação de Bash: Introdução)
- http://tldp.org/LDP/abs/html/index.html— Advanced Bash-Scripting Guide (Guia Avançado de Criação de Scripts Bash)
- http://www.grymoire.com/Unix/Sh.html— Sh - the Bourne Shell (Sh: o Bourne Shell)

9 Using Third-Party Software

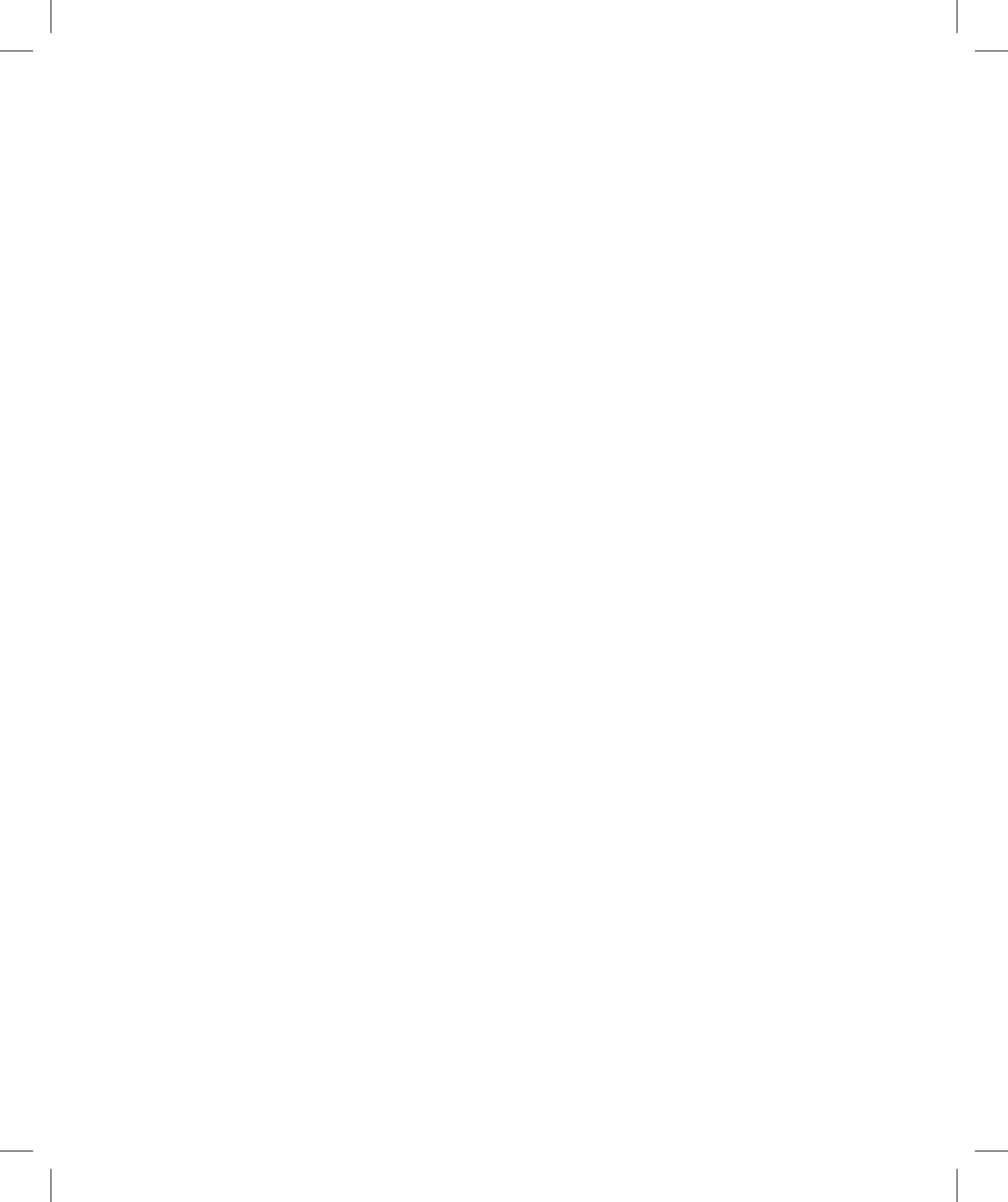
For information about using third-party software installed on SUSE Linux Enterprise and support of SUSE products used with third-party software, see the following links:

SUSE Partner Engineering Services Partner Certification Support Agreement
: https://www.suse.com/partners/ihv/yes/partner_engineering_services.html

Partner Software Catalog
: https://www.suse.com/susePSC/home

YES Certified Eligible Operating Systems
: https://www.suse.com/partners/ihv/yes/yes-certified-eligible-operating-systems.html

SUSE SolidDriver Program
: http://drivers.suse.com/doc/SolidDriver/

Independent Software Vendors
: https://www.suse.com/partners/isv/

SUSE Technical Support Handbook
: https://www.suse.com/support/handbook/

FAQ Support
: https://www.suse.com/support/faq.html

Parte II. Sistema

Aplicativos de 32 bits e 64 bits em um ambiente de sistema de 64 bits

10

O SUSE® Linux Enterprise Desktop está disponível para plataformas de 64 bits. Isso não significa necessariamente que todos os aplicativos incluídos tenham sido transpostos para plataformas de 64 bits. O SUSE Linux Enterprise Desktop suporta o uso de aplicativos de 32 bits em um ambiente de sistema de 64 bits. Este capítulo apresenta uma breve visão geral de como este suporte é implementado em plataformas de 64 bits do SUSE Linux Enterprise Desktop. Ele explica como aplicativos de 32 bits são executados (suporte do tempo de execução) e como aplicativos de 32 bits devem ser compilados para que possam ser executados em ambientes de sistema de 32 bits e 64 bits. Além disso, você encontrará informações sobre a API do kernel e uma explicação sobre como os aplicativos de 32 bits podem ser executados em um kernel de 64 bits.

O SUSE Linux Enterprise Desktop para as plataformas de 64 bits amd64 e Intel 64 foi desenvolvido para que os aplicativos de 32 bits existentes sejam executados no ambiente de 64 bits "out-of-the-box." Este suporte significa que você pode continuar a usar os aplicativos de 32 bits de sua preferência sem esperar que uma porta de 64 bits correspondente se torne disponível.

10.1 Suporte ao tempo de execução

IMPORTANTE: conflitos entre versões de aplicativos

Se um aplicativo estiver disponível para ambientes de 32 bits e de 64 bits, a instalação paralela das duas versões provavelmente resultará em problemas. Em tais casos, opte pela instalação e pelo uso de uma das duas versões.

Uma exceção a essa regra é o PAM (módulo de autenticação conectável). O SUSE Linux Enterprise Desktop usa o PAM no processo de autenticação como uma camada mediadora entre o usuário e o aplicativo. Em um sistema operacional de 64 bits que também executa aplicativos de 32 bits, é necessário sempre instalar as duas versões de um módulo PAM.

Para que os aplicativos sejam executados corretamente, cada um deles requer uma variedade de bibliotecas. Infelizmente, os nomes das versões de 32 bits e 64 bits das bibliotecas são idênticos. Eles devem ser diferenciados uns dos outros de outra forma.

Para obter compatibilidade com a versão de 32 bits, as bibliotecas são armazenadas no mesmo local no sistema e no ambiente de 32 bits. A versão de 32 bits de `libc.so.6` está localizada em `/lib/libc.so.6` nos ambientes de 32 bits e 64 bits.

Todos os arquivos de objetos e todas as bibliotecas de 64 bits estão localizados em diretórios denominados `lib64`. Os arquivos de objeto de 64 bits, que normalmente são encontrados em `/lib` e em `/usr/lib`, agora estão em `/lib64` e em `/usr/lib64`. Isso significa que há espaço para as bibliotecas de 32 bits em `/lib` e em `/usr/lib`, permitindo que o nome de arquivo de ambas as versões permaneça sem mudanças.

Os subdiretórios dos diretórios `/lib` de 32 bits com conteúdo de dados que não depende do tamanho do texto não são movidos. Este esquema está em conformidade com a LSB (Linux Standards Base — Base de Padrões Linux) e com o FHS (File System Hierarchy Standard — Padrão de Hierarquia de Sistema de Arquivos).

10.2 Desenvolvimento de software

Uma cadeia de ferramentas de desenvolvimento biarch permite a geração de objetos de 32 bits e 64 bits. O padrão é compilar objetos de 64 bits. É possível gerar objetos de 32 bits usando sinalizadores especiais. Para GCC, o sinalizador especial é `-m32`.

Todos os arquivos de cabeçalho devem ser escritos em um formato independente de arquitetura. As bibliotecas de 32 bits e 64 bits instaladas devem ter uma API (application programming interface — interface de programação de aplicativo) que corresponda aos arquivos de cabeçalho instalados. O ambiente normal do SUSE Linux Enterprise Desktop foi desenvolvido de acordo com este princípio. No caso de bibliotecas atualizadas manualmente, solucione esses problemas por conta própria.

10.3 Compilação de software em plataformas biarch

Para desenvolver binários para outra arquitetura em uma arquitetura biarch, as respectivas bibliotecas da segunda arquitetura devem ser instaladas adicionalmente. Esses pacotes são chamados de `rpmname-32bit`. Você também precisará dos respectivos cabeçalhos e bibliotecas dos pacotes `rpmname-devel` e das bibliotecas de desenvolvimento para a segunda arquitetura de `rpmname-devel-32bit`.

A maioria dos programas de código-fonte aberto usa uma configuração de programa baseada em `autoconf`. Para usar o `autoconf` com o objetivo de configurar um programa para a segunda arquitetura, sobregrave as configurações do compilador normal e do linker de `autoconf` executando o script `configure` com variáveis de ambiente adicionais.

O exemplo a seguir refere-se a um sistema x86_64 com x86 como a segunda arquitetura.

1 Use o compilador de 32 bits:

```
CC="gcc -m32"
```

2 Instrua o linker a processar objetos de 32 bits (use sempre `gcc` como o front end do linker):

```
LD="gcc -m32"
```

3 Defina o assembler para gerar objetos de 32 bits:

```
AS="gcc -c -m32"
```

4 Especifique flags do linker, como o local das bibliotecas de 32 bits, por exemplo:

```
LDFLAGS="-L/usr/lib"
```

5 Especifique o local das bibliotecas de código objeto de 32 bits:

```
--libdir=/usr/lib
```

6 Especifique o local das bibliotecas X de 32 bits:

```
--x-libraries=/usr/lib
```

Nem todas essas variáveis são necessárias para todos os programas. Adapte-as para o respectivo programa.

```
CC="gcc -m32"
LDFLAGS="-L/usr/lib;"
./configure --prefix=/usr --libdir=/usr/lib --x-libraries=/usr/lib
make
make install
```

10.4 Especificações do kernel

Os kernels de 64 bits para o x86_64 oferecem uma ABI (interface binária de aplicativo) para kernel de 64 bits e de 32 bits. A de 64 bits é idêntica à ABI do kernel de 32 bits correspondente. Isso significa que o aplicativo de 32 bits pode se comunicar com o kernel de 64 bits da mesma forma que com o kernel de 32 bits.

A emulação de 32 bits de chamadas do sistema para um kernel de 64 bits não suporta todas as APIs usadas pelos programas do sistema. Isso depende da plataforma. Por isso, alguns poucos aplicativos, como o `lspci`, precisam ser compilados..

Um kernel de 64 bits só pode carregar módulos de kernel de 64 bits especificamente compilados para esse kernel. Não é possível usar módulos de kernel de 32 bits.

DICA: Módulos carregáveis pelo Kernel

Alguns aplicativos requerem módulos separados carregáveis pelo kernel. Se você pretende usar um aplicativo de 32 bits desse tipo em um ambiente de sistema de 64 bits, entre em contato com o provedor do aplicativo e do SUSE para verificar se a versão de 64 bits do módulo carregável pelo kernel e a versão compilada de 32 bits da API do kernel estão disponíveis para esse módulo.

Inicializando e configurando um sistema Linux

11

O boot de um sistema Linux envolve componentes diferentes. O próprio hardware é inicializado pelo BIOS, que inicia o Kernel por meio de um carregador de boot. Depois disso, o processo de boot com `init` e os níveis de execução são totalmente controlados pelo sistema operacional. O conceito de nível de execução permite que você mantenha configurações para uso diário, e também execute tarefas de manutenção no sistema.

11.1 Processo de boot do Linux

O processo de boot do Linux consiste em vários estágios, cada um deles representado por um componente diferente. A lista a seguir resume o processo de boot e apresenta todos os principais componentes envolvidos.

1. **BIOS** Após ligar o computador, o BIOS inicializa a tela e o teclado e testa a memória principal. Até esse estágio, a máquina não acessa nenhuma mídia de armazenamento em massa. Em seguida, as informações sobre a data e o horário atuais e sobre os periféricos mais importantes são carregadas dos valores do CMOS. Quando o primeiro disco rígido e sua geometria são reconhecidos, o controle do sistema passa do BIOS para o carregador de boot.

2. **Carregador de boot** O primeiro setor de dados físico de 512 bytes do primeiro disco rígido é carregado na memória principal e o *carregador de boot* existente no início desse setor assume o controle. Os comandos executados pelo carregador de boot determinam a parte restante do processo de boot. Desse modo, os primeiros 512 bytes do primeiro disco rígido são chamados de MBR *(Master Boot Record)*. O carregador de boot passa o controle para o sistema operacional real, neste caso, o

Kernel do Linux. Mais informações sobre o GRUB, o carregador de boot do Linux, podem ser encontradas no Capítulo 12, *O carregador de boot GRUB* (p 143).

3. **Kernel e `initramfs`** Para passar o controle do sistema, o carregador de boot carrega na memória o kernel e um sistema de arquivos inicial baseado em RAM (`initramfs`). O conteúdo do `initramfs` pode ser usado diretamente pelo Kernel. O `initramfs` contém um pequeno executável chamado `init` que faz a montagem do sistema de arquivos raiz real. Se forem necessários drivers de hardware especiais para acessar o armazenamento em massa, eles deverão estar em `initramfs`. Para obter mais informações sobre o `initramfs`, consulte a Seção 11.1.1, "`initramfs`" (p 126).

4. **init no initramfs** Este programa executa todas as ações necessárias para montar o sistema de arquivos raiz apropriado, por exemplo, passar a funcionalidade de Kernel para o sistema de arquivos e os drivers de dispositivo necessários aos controladores de armazenamento em massa com `udev`. Uma vez encontrado o sistema de arquivos raiz, ele é verificado quanto a erros e montado. Se esse procedimento for bem-sucedido, o `initramfs` será limpo e o programa `init` no sistema de arquivos raiz será executado. Para obter mais informações sobre o `init`, consulte a Seção 11.1.2, "init no `initramfs`" (p 128). Há mais informações a respeito do `udev` no Capítulo 16, *Gerenciamento dinâmico de dispositivos do Kernel com `udev`* (p 209).

5. **`init`** O `init` realiza a inicialização do sistema em diversos níveis, oferecendo funcionalidades diferentes. O `init` está descrito na Seção 11.2, "O processo do `init`" (p 129).

11.1.1 `initramfs`

`initramfs` é um pequeno arquivo cpio que pode ser carregado pelo Kernel em um disco RAM. Ele fornece um ambiente Linux mínimo que permite a execução de programas antes da montagem do sistema de arquivos raiz. Esse ambiente Linux mínimo é carregado na memória pelas rotinas de BIOS e não têm requisitos de hardware específicos, além de memória suficiente. O `initramfs` deve sempre fornecer um executável chamado `init` que deve executar o programa `init` real no sistema de arquivos raiz para a continuação do processo de boot.

Antes da montagem do sistema de arquivos raiz e da inicialização do sistema operacional, o Kernel precisa dos drivers correspondentes para acessar o dispositivo em que o sistema de arquivos raiz está localizado. Esses drivers podem incluir drivers especiais para determinados tipos de unidades de disco rígido ou até drivers de rede para acesso a um sistema de arquivos de rede. Os módulos necessários para o sistema de arquivos raiz podem ser carregados pelo `init` no `initramfs`. Depois de carregados os módulos, o `udev` fornecerá os dispositivos necessários ao `initramfs`. Posteriormente no processo de boot, depois de mudar o sistema de arquivos raiz, será necessário gerar novamente os dispositivos. Isso é feito através de `boot.udev` com o comando `udevtrigger`.

Se você precisar mudar o hardware (por exemplo, discos rígidos) em um sistema instalado e esse hardware necessitar da presença de drivers diferentes no Kernel durante o boot, será necessário atualizar o `initramfs`. Isso é feito da mesma maneira que com seu antecessor, `init`, chamando o `mkinitrd`. A chamada de `mkinitrd sem argumentos cria um initramfs`. Chamar o `mkinitrd -R` cria um `init`. No SUSE® Linux Enterprise Desktop, os módulos a serem carregados são especificados pela variável `INITRD_MODULES` no `/etc/sysconfig/kernel`. Após a instalação, essa variável é definida automaticamente para o valor correto. Os módulos são carregados na mesma ordem em que são exibidos em `INITRD_MODULES`. Isso só é importante quando você depende da configuração correta dos arquivos de dispositivo `/dev/sd ?`. No entanto, em sistemas atuais, também é possível usar os arquivos de dispositivo em `/dev/disk/` que são classificados em vários subdiretórios, chamados `by-id`, `by-path` e `by-uuid`, e que sempre representam o mesmo disco. Isso também é possível na hora da instalação, especificando a respectiva opção de montagem.

IMPORTANTE: Atualizando o `initramfs` ou o `init`

O carregador de boot carrega o `initramfs` ou o `init` da mesma maneira que o Kernel. Não é necessário reinstalar o GRUB após atualizar o `initramfs` ou o `init`, pois o GRUB procura o arquivo correto no diretório durante a inicialização.

11.1.2 init no `initramfs`

O principal objetivo do `init` no `initramfs` é preparar a montagem e o acesso ao sistema de arquivos raiz real. Dependendo da configuração do sistema, o `init` será responsável pelas tarefas a seguir.

Carregamento de módulos Kernel
: Dependendo da configuração do seu hardware, drivers especiais podem ser necessários para acessar os componentes de hardware do computador (sendo que o componente mais importante é a unidade de disco rígido). Para acessar o sistema de arquivos raiz final, o Kernel precisa carregar os drivers adequados do sistema de arquivos.

Fornecendo arquivos especiais de bloco
: Para cada módulo carregado, o Kernel gera eventos de dispositivo. O `udev` gerencia esses eventos e gera os arquivos de bloco especiais necessários em um sistema de arquivos RAM em `/dev`. Sem esses arquivos especiais, o sistema de arquivos e outros dispositivos não estariam acessíveis.

Gerenciamento de configurações RAID e LVM
: Se você tiver configurado o sistema para armazenar o sistema de arquivos raiz no RAID ou no LVM, o `init` configurará o LVM ou o RAID para permitir acesso posterior ao sistema de arquivos raiz. Obtenha informações sobre RAID e LVM no Chapter 12, *Advanced Disk Setup* (↑*Deployment Guide*).

Gerenciamento de conexões de rede
: Se você tiver configurado o sistema para usar um sistema de arquivos raiz montado em rede (via NFS), o `init` deverá verificar se os drivers de rede corretos foram carregados e estão configurados para permitir acesso ao sistema de arquivos raiz.

Quando o `init` é chamado durante o boot inicial como parte do processo de instalação, suas tarefas são diferentes das que foram mencionadas acima:

Localização da mídia de instalação
: Quando o processo de instalação é iniciado, a máquina carrega um Kernel de instalação e um `init` especial com o instalador do YaST no meio de instalação. O instalador do YaST, executado em um sistema de arquivos RAM, precisa ter

informações sobre a localização do meio de instalação para acessá-lo e instalar o sistema operacional.

Inicialização do reconhecimento de hardware e carregamento dos módulos kernel adequados

Como mencionado na Seção 11.1.1, “initramfs” (p 126), o processo de boot é iniciado com um conjunto mínimo de drivers que pode ser usado com a maioria das configurações de hardware. O init inicia um processo de exploração de hardware que determina o conjunto de drivers adequado à sua configuração de hardware. Os nomes dos módulos necessários ao processo de boot são gravados em INITRD_MODULES, localizado em /etc/sysconfig/kernel. Esses nomes são usados para gerar um initramfs personalizado necessário para inicializar o sistema. Se os módulos não forem necessários para o boot, mas forem para coldplug, eles serão gravados em /etc/sysconfig/hardware/hwconfig-*. Todos os dispositivos descritos com arquivos de configuração nesse diretório são inicializados durante o processo de boot.

Carregamento do sistema de instalação ou do sistema de recuperação

Assim que o hardware for reconhecido apropriadamente, os drivers adequados serão carregados, o udev criará os arquivos de dispositivos especiais e o init iniciará o sistema de instalação com o instalador real do YaST ou o sistema de recuperação.

Inicialização do YaST

Por fim, o init inicia o YaST, que inicia a instalação do pacote e a configuração do sistema.

11.2 O processo do init

O programa init tem ID de processo 1. Ele é responsável por inicializar o sistema da maneira necessária. O init é iniciado diretamente pelo Kernel e resiste ao sinal 9, que normalmente elimina processos. Todos os outros programas são iniciados diretamente pelo init ou por um de seus processos filho.

O init é configurado centralmente no arquivo /etc/inittab em que os *níveis de execução* são definidos (consulte a Seção 11.2.1, “Níveis de execução” (p 130)). O arquivo também especifica os serviços e os daemons disponíveis em cada um dos níveis

de execução. Dependendo das entradas em /etc/inittab, vários scripts são executados pelo init. Por padrão, o primeiro script iniciado após o boot é o /etc/init.d/boot. Após concluída a fase de inicialização do sistema, o nível de execução do sistema muda para o padrão com o script /etc/init.d/rc. Para fins de clareza, esses scripts, chamados *scripts init*, residem no diretório /etc/init.d (consulte a Seção 11.2.2, “Scripts Init” (p 133)).

Todo o processo de inicialização e encerramento do sistema é mantido pelo init. Desse ponto de vista, o Kernel pode ser considerado um processo em segundo plano para manter todos os outros processos e ajustar o tempo de CPU e o acesso ao hardware de acordo com as solicitações de outros programas.

11.2.1 Níveis de execução

No Linux, os *níveis de execução* definem como o sistema é iniciado e quais serviços estão disponíveis no sistema em execução. Após o boot, o sistema é iniciado conforme definido em /etc/inittab na linha initdefault. Normalmente, é 3 ou 5. Consulte a Tabela 11.1, “Níveis de execução disponíveis” (p 130). Como alternativa, é possível especificar o nível de execução durante o boot (adicionando o número do nível de execução no prompt de boot, por exemplo). Os parâmetros que não forem avaliados diretamente pelo próprio Kernel serão passados para o init. Para inicializar no nível de execução 3, adicione o número 3 ao prompt de boot.

Tabela 11.1 *Níveis de execução disponíveis*

Nível de execução	Descrição
0	Desligamento do sistema
S ou 1	Modo de usuário único
2	Modo multiusuário local sem rede remota (NFS, etc.)
3	Modo multiusuário completo com rede

Nível de execução	Descrição
4	*Definido pelo Usuário*, não usado a menos que o administrador configure este nível de execução.
5	Modo multiusuário completo com rede e gerenciador de vídeo X — KDM, GDM ou XDM
6	Reinicialização do sistema

IMPORTANTE: evite o Nível de execução 2 com uma partição montada via NFS

Você não deverá usar o nível de execução 2 se seu sistema montar uma partição como `/usr` através do NFS. O sistema pode comportar-se de forma inesperada se as bibliotecas ou arquivos de programa estiverem ausentes pois o serviço NFS não está disponível no nível de execução 2 (modo multiusuário local sem rede remota).

Para mudar os níveis de execução durante a execução do sistema, digite `telinit` e o número correspondente como um argumento. Somente o administrador do sistema pode fazer isso. A lista a seguir resume os comandos mais importantes na área de nível de execução.

`telinit 1` ou `shutdown now`
: O sistema muda para o *modo de usuário único*. Esse modo é usado para manutenção do sistema e tarefas de administração.

`telinit 3`
: Todos os programas e serviços essenciais (incluindo a rede) são iniciados, e os usuários comuns podem efetuar login e trabalhar no sistema sem um ambiente gráfico.

`telinit 5`
: O ambiente gráfico é habilitado. Geralmente um gerenciador de exibição como XDM, GDM ou KDM é iniciado. Se o login automático estiver habilitado, o usuário

local será conectado ao gerenciador de janelas pré-selecionado (GNOME ou KDE ou qualquer outro gerenciador de janelas).

`telinit 0` ou `shutdown -h now`
: O sistema é desligado.

`telinit 6` ou `shutdown -r now`
: O sistema é desligado e, em seguida, reinicializado.

Nível de Execução `5` é o nível de execução padrão em todas as instalações padrão do SUSE Linux Enterprise Desktop. É solicitado o login dos usuários com uma interface gráfica ou o usuário padrão está conectado automaticamente.

ATENÇÃO: Erros em `/etc/inittab` podem resultar em um boot de sistema com falha

Se `/etc/inittab` for danificado, o sistema poderá não ser inicializado adequadamente. Portanto, seja extremamente cuidadoso ao editar `/etc/inittab`. Sempre deixe que o `init` leia novamente `/etc/inittab` com o comando `telinit q` antes de reinicializar a máquina.

Geralmente, há duas situações quando os níveis de execução são mudados. Primeiro, os scripts de parada do nível de execução atual são iniciados, fechando alguns programas essenciais ao nível de execução atual. Em seguida, os scripts do novo nível de execução são iniciados. Na maioria dos casos, vários programas são iniciados. Por exemplo, ocorre o seguinte quando o nível de execução 3 muda para 5:

1. O administrador (`root`) solicita que o init mude para um nível de execução diferente digitando `telinit 5`.

2. O init verifica o nível de execução atual (`runlevel`) e determina se ele deve iniciar `/etc/init.d/rc` com o novo nível de execução como parâmetro.

3. Agora, `rc` chama os scripts de parada do nível de execução atual para os quais não há script de início no novo nível de execução. Neste exemplo, todos os scripts residem em `/etc/init.d/rc3.d` (o nível de execução antigo era 3) e iniciam com `K`. O número após `K` especifica a ordem de execução dos scripts com o parâmetro `stop`, pois algumas dependências devem ser consideradas.

4. Os scripts do novo nível de execução são os últimos a serem iniciados. Neste exemplo, eles estão em /etc/init.d/rc5.d e começam com S. Mais uma vez, o número após S determina a sequência de início dos scripts.

Ao mudar para o mesmo nível de execução que o atual, o init somente verifica as mudanças em /etc/inittab e inicia as etapas apropriadas, por exemplo, para iniciar um getty em outra interface. A mesma funcionalidade pode ser obtida com o comando telinit q.

11.2.2 Scripts Init

Há dois tipos de scripts em /etc/init.d:

Scripts executados diretamente pelo init
: Isso só ocorrerá durante o processo de boot ou se for iniciado um encerramento imediato do sistema (falha de energia ou pressionamento de Ctrl + Alt + Del pelo usuário). A execução desses scripts é definida em /etc/inittab.

Scripts executados indiretamente pelo init
: São executados durante a mudança do nível de execução e sempre chamam o script master /etc/init.d/rc, que garante a ordem correta dos scripts relevantes.

Todos os scripts estão localizados em /etc/init.d. Scripts que são executados durante o boot são chamados através de links simbólicos de /etc/init.d/boot .d. Os scripts para mudança do nível de execução são chamados através de links simbólicos em um dos subdiretórios (/etc/init.d/rc0.d para /etc/init.d/ rc6.d). Isso só serve para fins de clareza, além de evitar scripts duplicados se forem usados em vários níveis de execução. Como todos os scripts podem ser executados como de início ou de parada, eles devem entender os parâmetros start e stop. Os scripts também entendem as opções restart, reload, force-reload e status. Essas diversas opções são explicadas na Tabela 11.2, “Opções possíveis do script init” (p 134). Os scripts executados diretamente pelo init não têm esses links. Eles são executados independentemente do nível de execução, quando necessário.

Tabela 11.2 Opções possíveis do script init

Opção	Descrição
`start`	Iniciar serviço.
`stop`	Interromper serviço.
`restart`	Se o serviço estiver sendo executado, vai pará-lo ou reiniciá-lo. Se não estiver, vai iniciá-lo.
`reload`	Recarregar a configuração sem parar e reiniciar o serviço.
`force-reload`	Recarregar a configuração se o serviço suportá-la. Caso contrário, age como se `restart` tivesse sido ativado.
`status`	Mostrar o status atual do serviço.

Os links em cada subdiretório específico de nível de execução possibilitam a associação de scripts a diferentes níveis de execução. Durante a instalação ou desinstalação de pacotes, esses links são adicionados e removidos com a ajuda do programa insserv (ou usando `/usr/lib/lsb/install_initd`, que é um script que chama esse programa). Consulte `man 8 insserv` para mais detalhes.

Todas essas configurações também podem ser mudadas com a ajuda do módulo do YaST. Se precisar verificar o status na linha de comando, use a ferramenta `chkconfig`, descrita na página de manual de `man 8 chkconfig`.

Veja a seguir uma pequena apresentação dos scripts de boot e de parada iniciados primeiro e por último, respectivamente, bem como uma explicação do script de manutenção.

`boot`
: `Executado na inicialização do sistema usando diretamente o init`. É independente do nível de execução escolhido e só é executado uma vez. Aqui, os sistemas de arquivos `/proc` e `/dev/pts` são montados, e `blogd`

(boot logging daemon — daemon de registro de boot) é ativado. Se o sistema for inicializado pela primeira vez após uma atualização ou instalação, a configuração inicial do sistema será iniciada.

O daemon `blogd` é um serviço iniciado por `boot` e `rc` antes de qualquer outro. Ele é interrompido após a conclusão das ações acionadas por esses scripts (que executam vários subscripts, por exemplo, disponibilizando arquivos de bloco especiais). blogd grava qualquer saída de tela no arquivo de registro `/var/log/boot.msg`, mas somente se e quando `/var` for montado como leitura-gravação. Caso contrário, o blogd armazenará no buffer todos os dados de tela até que `/var` se torne disponível. Obtenha mais informações sobre o `blogd` com `man 8 blogd`.

O script `boot` também é responsável pela inicialização de todos os scripts em `/etc/init.d/boot.d` cujos nomes começam com `S`. Nesse local, todos os sistemas de arquivos são verificados e os dispositivos de loop são configurados se necessário. O horário do sistema também é definido. Se ocorrer um erro durante a verificação e o reparo automáticos do sistema de arquivos, o administrador do sistema poderá intervir após digitar a senha raiz. O último script executado é `boot.local`.

`boot.local`
: Digite aqui comandos adicionais a serem executados na inicialização antes de mudar para um nível de execução. Ele pode ser comparado ao `AUTOEXEC.BAT` em sistemas DOS.

`halt`
: Esse script é executado apenas ao mudar para o nível de execução 0 ou 6. Aqui, ele é executado como `init` ou como `init`. O modo como `halt` é chamado determina se o sistema deve ser encerrado ou reinicializado. Se houver necessidade de comandos especiais durante o encerramento, adicione-os ao script `init`.

`rc`
: Este script chama os scripts de parada adequados do nível de execução atual e os scripts de início do nível de execução recém-selecionado. Assim como o script `/etc/init.d/boot`, esse script é chamado de `/etc/inittab` com o nível de execução desejado como parâmetro.

Você pode criar seus próprios scripts e integrá-los facilmente no esquema descrito acima. Para obter instruções sobre como formatar, nomear e organizar scripts personalizados, consulte as especificações do LSB e as páginas de manual de `init`, `init.d`, `chkconfig` e `insserv`. Além disso, consulte as páginas de manual do `startproc` e `killproc`.

ATENÇÃO: Scripts Init com falha podem desligar o sistema

Scripts `init` com falha podem desligar sua máquina. Edite esses scripts com muito cuidado e, se possível, submeta-os a testes detalhados no ambiente multiusuário. Encontre informações úteis sobre scripts `init` na Seção 11.2.1, “Níveis de execução” (p 130).

Para criar um script `init` personalizado para determinado programa ou serviço, use o arquivo `/etc/init.d/skeleton` como modelo. Grave uma cópia desse arquivo com o novo nome e edite o programa relevante e nomes de arquivos, caminhos e outros detalhes necessários. Você também pode precisar aprimorar o script com suas próprias partes, de modo que as ações corretas sejam acionadas pelo procedimento `init`.

O bloco `INIT INFO` na parte superior é uma parte necessária do script e deve ser editada. Consulte o Exemplo 11.1, “Um bloco INIT INFO mínimo” (p 136).

Exemplo 11.1 *Um bloco INIT INFO mínimo*

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

Na primeira linha do bloco `INFO`, após `Provides:`, especifique o nome do programa ou serviço controlado pelo script init. Nas linhas `Required-Start:` e `Required-Stop:`, especifique todos os serviços que precisam continuar em execução quando o próprio serviço for interrompido. Essas informações são usadas posteriormente para gerar a numeração dos nomes de script, como encontrada nos diretórios de nível de execução. Depois de `Default-Start:` e `Default-Stop:`, especifique os níveis de execução em que o serviço deve ser iniciado ou parado automaticamente. Por fim, para `Description:`, forneça uma breve descrição do serviço em questão.

Para criar os links dos diretórios de nível de execução (`/etc/init.d/rc?.d/`) para os scripts correspondentes em `/etc/init.d/`, digite o comando `insserv` *`new-script-name`*. `insserv` avalia o cabeçalho `INIT INFO` para criar os links necessários aos scripts de início e parada nos diretórios de nível de execução (`/etc/init.d/rc?.d/`). O programa também se encarrega da ordem correta de início e parada para cada nível de execução, incluindo os números necessários nos nomes desses links. Se você preferir uma ferramenta gráfica para criar esses links, use o editor de runlevel fornecido pelo YaST, como descrito na Seção 11.2.3, "Configurando serviços do sistema (runlevel) com o YaST" (p 137).

Se um script já existir em `/etc/init.d/`, deve ser integrado ao esquema de runlevel existente. Crie os links nos diretórios de runlevel imediatamente com insserv ou por meio do serviço correspondente no editor de runlevel do YaST. As mudanças serão aplicadas durante a próxima reinicialização, e o novo serviço será iniciado automaticamente.

Não defina esses links manualmente. Se houver algum erro no bloco `INFO`, surgirão problemas quando `insserv` for executado posteriormente para algum outro serviço. O serviço adicionado manualmente será removido na próxima execução de `insserv` para esse script.

11.2.3 Configurando serviços do sistema (runlevel) com o YaST

Depois que o módulo do YaST é iniciado em *YaST* > *Sistema* > *Serviços do Sistema (Nível de Execução)*, ele exibe uma visão geral que lista todos os serviços disponíveis e o status atual de cada um deles (desabilitado ou habilitado). Decida se o módulo deve ser usado no *Modo Simples* ou no *Modo de Especialista*. O *Modo Simples* padrão deve ser suficiente na maior parte dos casos. A coluna à esquerda mostra o nome do serviço, a coluna ao centro indica seu status atual e a coluna à direita fornece uma descrição resumida. Para o serviço selecionado, uma descrição mais detalhada é fornecida na parte inferior da janela. Para habilitar um serviço, selecione-o na tabela e, em seguida, selecione *Habilitar*. As mesmas etapas se aplicam para desabilitar um serviço.

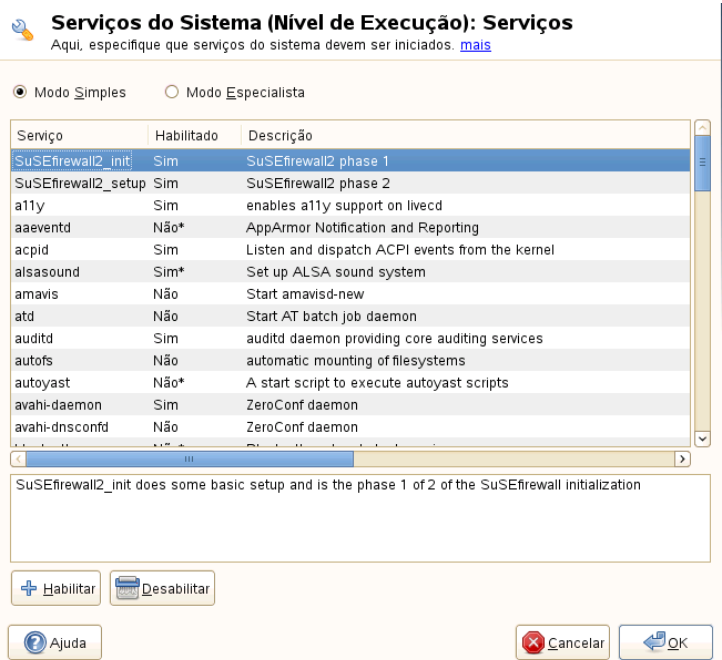
Para ter mais controle sobre os níveis de execução em que um serviço é iniciado ou parado ou para mudar o nível de execução padrão, selecione primeiro *Modo de Especialista*. O nível de execução padrão atual ou o "initdefault" (o nível de execução

em que o sistema é inicializado por padrão) é exibido na parte superior. Normalmente, o nível de execução padrão de um sistema SUSE Linux Enterprise Desktop é o 5 (modo multiusuário completo com rede e X). Uma alternativa adequada poderia ser o nível de execução 3 (modo multiusuário completo com rede).

Esta caixa de diálogo do YaST permite a seleção de um dos runlevels (como listado na Tabela 11.1, "Níveis de execução disponíveis" (p 130)) como o novo padrão. Além disso, use a tabela mostrada nessa janela para habilitar ou desabilitar serviços e daemons individuais. A tabela lista os serviços e daemons disponíveis, mostra se eles estão habilitados no sistema e, se estiverem, para quais níveis de execução. Após selecionar uma das linhas com o mouse, clique nas caixas de seleção que representam os níveis de execução (*B*, *0*, *1*, *2*, *3*, *5*, *6* e *S*) para definir os níveis de execução em que o serviço ou daemon selecionado deve estar em execução. O nível de execução 4 é indefinido para permitir a criação de um nível de execução personalizado. Uma breve descrição do serviço ou daemon selecionado no momento é fornecida abaixo da visão geral da tabela.

ATENÇÃO: Configurações de nível de execução defeituosas podem danificar o sistema

Configurações de nível de execução defeituosas podem tornar o sistema inutilizável. Antes de aplicar as mudanças, tenha absoluta certeza sobre suas consequências.

Figura 11.1 Serviços do Sistema (Nível de Execução)

Com *Iniciar, Parar ou Atualizar*, decida se um serviço deve ser ativado. *Situação da Renovação* verifica o status atual. *Inicializar/Reinicializar* permite selecionar se você deseja aplicar as mudanças ao sistema ou restaurar as configurações existentes antes de inicializar o editor de nível de execução. Selecione *OK* para gravar as configurações modificadas no disco.

11.3 Configuração do sistema via /etc/sysconfig

A configuração principal do SUSE Linux Enterprise Desktop é controlada pelos arquivos de configuração em `/etc/sysconfig`. Os arquivos individuais em `/etc/sysconfig` são lidos somente pelos scripts para os quais são relevantes. Isso garante que as configurações de rede, por exemplo, somente precisem ser analisadas pelos scripts relacionados à rede.

Há duas maneiras de editar a configuração do sistema. Use o Editor sysconfig do YaST ou edite manualmente os arquivos de configuração.

11.3.1 Mudando a configuração do sistema usando o Editor sysconfig do YaST

O editor sysconfig do YaST dispõe de um front end fácil de usar para a configuração do sistema. Sem conhecimento do local real da variável de configuração que precisa ser mudada, você pode apenas usar a função de pesquisa incorporada desse módulo, mudar o valor dessa variável conforme necessário e permitir que o YaST se encarregue de aplicar essas mudanças, atualizando as configurações que dependem dos valores definidos no `sysconfig` e reiniciando os serviços.

ATENÇÃO: A modificação dos arquivos `/etc/sysconfig/*` pode danificar a instalação

Não modifique os arquivos `/etc/sysconfig` se você não tiver experiência e conhecimento prévios. Isso pode causar sérios danos ao sistema. Os arquivos em `/etc/sysconfig` contêm um pequeno comentário sobre cada variável para explicar seu efeito real.

Figura 11.2 *Configuração do sistema usando o Editor sysconfig*

A caixa de diálogo do Editor sysconfig do YaST é divida em três partes. A parte esquerda mostra uma tela de árvore de todas as variáveis configuráveis. Quando você seleciona uma variável, a parte direita exibe a seleção e a definição atuais dessa variável. Abaixo, uma terceira janela exibe uma descrição resumida da finalidade da variável, os valores possíveis, o valor padrão e o arquivo de configuração do qual essa variável se origina. A caixa de diálogo também fornece informações sobre qual script de configuração é executado após a mudança da variável e qual novo serviço é iniciado como resultado da mudança. O YaST solicita a confirmação das mudanças e informa quais scripts serão executados depois que você sair da caixa de diálogo selecionando *Concluir*. Além disso, selecione os serviços e scripts que devem ser ignorados agora e iniciados mais tarde. O YaST aplica todas as mudanças automaticamente e reinicia os serviços envolvidos para que elas sejam efetivadas.

11.3.2 Mudando manualmente a configuração do sistema

Para mudar manualmente a configuração do sistema, faça o seguinte

1 Torne-se `root`.

2 Coloque o sistema no modo de usuário único (nível de execução 1) com `telinit 1`.

3 Mude os arquivos de configuração, conforme o necessário, com um editor de sua preferência.

   Se você não usar o YaST para mudar os arquivos de configuração em `/etc/sysconfig`, verifique se os valores das variáveis vazias estão representados por duas aspas (`KEYTABLE=""`) e se os valores com espaços em branco estão entre aspas. Os valores constituídos de somente uma palavra não precisam ficar entre aspas.

4 Execute `SuSEconfig` para verificar se as mudanças foram efetivadas.

5 Coloque o sistema de volta no nível de execução anterior com o comando `telinit` *`nível_de_execução_padrão`*. Substitua *`nível_de_execução_padrão`* pelo nível de execução padrão do sistema. Escolha `5` para retornar ao modo

multiusuário completo com rede e X ou escolha `3` se preferir trabalhar no modo multiusuário completo com rede.

Esse procedimento é relevante principalmente durante a mudança das configurações em todo o sistema, como a configuração da rede. Pequenas mudanças não devem requerer alternar para o modo de usuário único, mas você pode fazer isso para ter certeza de que todos os programas em questão foram reiniciados corretamente.

DICA: definindo a configuração automatizada do sistema

Para desabilitar a configuração automatizada do sistema pelo SuSEconfig, defina a variável `ENABLE_SUSECONFIG` em `/etc/sysconfig/suseconfig` como `no`. Não desabilite o SuSEconfig se quiser usar o suporte de instalação do SUSE. Também é possível desabilitar parcialmente a configuração automática.

O carregador de boot GRUB 12

Este capítulo descreve como configurar o GRUB (Grand Unified Bootloader), o carregador de boot usado no SUSE® Linux Enterprise Desktop. Há um módulo especial do YaST disponível para ajustar todas as configurações. Se você não estiver familiarizado com a ideia de entrar para o Linux, leia as seções a seguir para obter algumas informações de apoio. Este capítulo também descreve alguns problemas frequentemente encontrados quando se inicializa com o GRUB e mostra as soluções para eles.

NOTA: Ausência do GRUB em máquinas que usam UEFI

Sistematicamente, o GRUB é instalado em máquinas equipadas com BIOS tradicional e em máquinas com UEFI (Unified Extensible Firmware Interface) que usam um CSM (Compatibility Support Module — Módulo de Suporte de Compatibilidade). Em máquinas com UEFI sem CSM habilitado, o `eLILO` será instalado automaticamente (desde que o DVD1 tenha sido inicializado com êxito). Consulte a documentação do eLILO em `/usr/share/doc/packages/elilo/` no seu sistema para obter os detalhes.

Este capítulo se concentra no gerenciamento de boot e na configuração do carregador de boot do GRUB. O procedimento de boot como um todo é detalhado no Capítulo 11, *Inicializando e configurando um sistema Linux* (p 125). O carregador de boot representa a interface entre a máquina (BIOS) e o sistema operacional (SUSE Linux Enterprise Desktop). A configuração do carregador de boot influencia diretamente o boot do sistema operacional.

Os termos a seguir aparecem com frequência neste capítulo e talvez precisem de alguma explicação:

MBR (Master Boot Record)
A estrutura do MBR é definida por uma convenção que independe do sistema operacional. Os primeiros 446 bytes são reservados para o código do programa. Normalmente, eles contêm parte de um programa carregador de boot ou um seletor de sistema operacional. Os 64 bytes seguintes fornecem espaço para uma tabela de partição de até quatro entradas. A tabela de partição contém informações sobre o particionamento do disco rígido e sobre os tipos de sistema de arquivos. O sistema operacional precisa dessa tabela para lidar com o disco rígido. Com o código genérico convencional no MBR, exatamente uma partição deve ser marcada como *ativa*. Os dois últimos bytes do MBR devem conter um "número mágico" estático (`AA55`). Um MBR que contém um valor diferente é tido como inválido por alguns BIOS, não sendo considerado para o boot.

Setores de Boot
Os setores de boot são os primeiros setores das partições do disco rígido, com a execução da partição estendida, que serve meramente como "container" para outras partições. Esses setores de boot têm 512 bytes de espaço para o código usado para inicializar um sistema operacional instalado na partição respectiva. Isso se aplica aos setores de boot das partições DOS, Windows e OS/2 formatadas, que também contêm alguns dados básicos importantes do sistema de arquivos. Os setores de boot das partições Linux, ao contrário, ficam inicialmente vazias após a configuração de um sistema de arquivos diferente do XFS. Portanto, uma partição Linux não é inicializável por si mesma, mesmo que contenha um kernel e um sistema válido de arquivos raiz. Um setor de boot com código válido para inicializar o sistema tem o mesmo número mágico que o MBR em seus dois últimos bytes (`AA55`).

12.1 Inicializando com o GRUB

O GRUB é composto por duas fases. O Estágio 1 consiste em 512 bytes, e sua única tarefa é carregar o segundo estágio do carregador de boot. Consequentemente, a estágio 2 é carregado. Este estágio contém a parte principal do carregador de boot.

Em algumas configurações, um estágio intermediário 1.5 pode ser usado, que localiza e carrega o estágio 2 de um sistema de arquivos apropriado. Se possível, este método é escolhido por padrão durante a instalação ou durante a configuração inicial do GRUB com o YaST.

O estágio 2 consegue acessar vários sistemas de arquivos. Atualmente, são suportados o ext2, ext3, ReiserFS, Minix e o sistema de arquivos FAT do DOS usado pelo Windows. Até certo ponto, XFS, e UFS e FFS usados pelos sistemas BSD também são suportados. Desde a versão 0.95, o GRUB também pode ser inicializado de um CD ou DVD que contenha um sistema de arquivos padrão ISO 9660 de acordo com a especificação “El Torito”. Mesmo antes da inicialização do sistema, o GRUB pode acessar os sistemas de arquivos dos dispositivos de disco BIOS suportados (disquetes ou discos rígidos, unidades de CD e unidades de DVD detectados pelo BIOS). Portanto, as mudanças realizadas no arquivo de configuração do GRUB (`menu.lst`) não exigem uma nova instalação do gerenciador de boot. Quando o sistema é inicializado, o GRUB carrega o arquivo de menu com os caminhos e dados de partição válidos do kernel ou do disco RAM inicial (`initrd`) e localiza os arquivos.

A configuração real do GRUB baseia-se em quatro arquivos, que são descritos a seguir:

`/boot/grub/menu.lst`
: Este arquivo contém todas as informações sobre partições ou sistemas operacionais que podem ser inicializados com o GRUB. Sem essas informações, a linha de comando do GRUB pergunta ao usuário como proceder (consulte a Seção 12.1.1.3, “Editando as entradas de menu durante o procedimento de boot” (p 150) para obter detalhes).

`/boot/grub/device.map`
: Esse arquivo traduz os nomes dos dispositivos da notação do GRUB e do BIOS para os nomes de dispositivos do Linux.

`/etc/grub.conf`
: Esse arquivo contém os comandos, os parâmetros e as opções que o shell do GRUB precisa para instalar corretamente o carregador de boot.

`/etc/sysconfig/bootloader`
: Esse arquivo é lido pela biblioteca perl-bootloader, que é usada na configuração do carregador de boot com o YaST e sempre que um novo kernel é instalado. Ele inclui opções de configuração (como parâmetros do kernel) que são adicionadas por padrão ao arquivo de configuração do carregador de boot.

O GRUB pode ser controlado de várias maneiras. As entradas de boot de uma configuração existente podem ser selecionadas no menu gráfico (splash screen). A configuração é carregada a partir do arquivo `menu.lst`.

No GRUB, todos os parâmetros de boot podem ser alterados antes do boot. Por exemplo, os erros cometidos durante a edição do arquivo de menu podem ser corrigidos desta maneira. Os comandos de boot também podem ser inseridos de forma interativa em um tipo de prompt de entrada. Para obter os detalhes, consulte a Seção 12.1.1.3, "Editando as entradas de menu durante o procedimento de boot" (p 150). O GRUB oferece a possibilidade de determinar a localização do kernel e do `initrd` antes do boot. Dessa maneira, você pode até inicializar um sistema operacional instalado para o qual não existe entrada na configuração do carregador de boot.

Na verdade, o GRUB existe em duas versões: como carregador de boot e como programa normal do Linux em `/usr/sbin/grub`. O segundo é conhecido como *shell do GRUB*. Ele fornece uma emulação do GRUB no sistema instalado e pode ser usado para instalar o GRUB ou testar novas configurações antes de aplicá-las. A funcionalidade para instalar o GRUB como carregador de boot em um disco rígido ou em um disquete é integrada ao GRUB na forma do comando `setup`. Isso está disponível no shell do GRUB quando o Linux é carregado.

12.1.1 O arquivo /boot/grub/menu.lst

A tela de apresentação gráfica com o menu de boot baseia-se no arquivo de configuração do GRUB `/boot/grub/menu.lst`, que contém todas as informações sobre todas as partições ou sistemas operacionais que podem ser inicializados pelo menu.

Todas as vezes em que o sistema é inicializado, o GRUB carrega o arquivo de menu a partir do sistema de arquivos. Por essa razão, o GRUB não precisa ser reinstalado depois de todas as modificações no arquivo. Use o carregador de boot YaST para modificar a configuração do GRUB conforme descrito no Seção 12.2, "Configurando o carregador de boot com o YaST" (p 155).

O arquivo de menu contém comandos. A sintaxe é muito simples. Cada linha contém um comando seguido de parâmetros opcionais separados por espaços, como ocorre no shell. Por razões históricas, alguns comandos admitem um = na frente do primeiro parâmetro. Os comentários são introduzidos por um hash (`#`).

Para identificar os itens do menu na visão geral do menu, defina um `título` para cada entrada. O texto (incluindo os espaços) que vem depois da palavra-chave `título` é exibido como opção selecionável no menu. Todos os comandos até o próximo `título` são executados quando se seleciona esse item de menu.

O caso mais simples é o redirecionamento para os carregadores de boot de outros sistemas operacionais. O comando é `chainloader` e o argumento é geralmente o bloco de inicialização de outra partição na notação do bloco do GRUB. Por exemplo:

```
chainloader (hd0,3)+1
```

Os nomes de dispositivo no GRUB são explicados em Seção 12.1.1.1, "Convenções de nomeação para discos rígidos e partições" (p 148). Este exemplo especifica o primeiro bloco da quarta partição do primeiro disco rígido.

Use o comando `kernel` para especificar uma imagem do kernel. O primeiro argumento é o caminho para a imagem do kernel em uma partição. Os outros argumentos são passados para o kernel na linha de comando.

Se o kernel não contiver drivers incorporados para acesso à partição raiz ou um sistema Linux recente com recursos de hotplug avançados for usado, o `initrd` deve ser especificado com um comando separado do GRUB cujo único argumento é o caminho para o arquivo `initrd`. Como o endereço de carregamento do `initrd` é gravado na imagem do kernel carregado, o comando `initrd` deve vir imediatamente após o comando `kernel`.

O comando `root` simplifica a especificação do kernel e dos arquivos initrd. O único argumento de `root` é um dispositivo ou uma partição. Esse dispositivo é usado para todos os kernels, `initrd`, ou para outros caminhos de arquivo para os quais não há dispositivos explicitamente especificados até o próximo comando `root`.

O comando `boot` está implícito no fim de cada entrada do menu, assim ele não precisa ser gravado no arquivo de menu. No entanto, para usar o GRUB interativamente para o boot, você deve inserir o comando `boot` no final. O comando em si não tem argumentos. Ele meramente inicializa a imagem do kernel carregado ou do carregador de cadeia especificado.

Depois de gravar todas as entradas de menu, defina uma delas como entrada `default`. Do contrário, é utilizada a primeira (entrada `0`). Você também pode especificar um tempo de espera em segundos depois do qual a entrada default deve ser inicializada. `timeout` e `default` geralmente precedem as entradas de menu. Um arquivo de exemplo está descrito em Seção 12.1.1.2, "Um exemplo de arquivo de menu" (p 149).

12.1.1.1 Convenções de nomeação para discos rígidos e partições

As convenções de nomeação que o GRUB utiliza para discos rígidos e partições diferem daquelas usadas para os dispositivos Linux normais. Elas são mais parecidas com a enumeração de disco simples feita pelo BIOS, além disso, a sintaxe é semelhante à usada em alguns derivativos do BSD. No GRUB, a numeração das partições começa com zero. Isso significa que (hd0,0) é a primeira partição do primeiro disco rígido. Em uma máquina desktop comum, com um disco rígido conectado como master principal, o nome do dispositivo Linux correspondente é /dev/sda1.

As quatro partições principais possíveis são atribuídas aos números de partição de 0 a 3. As partições lógicas são numeradas a partir de 4:

```
(hd0,0)   first primary partition of the first hard disk
(hd0,1)   second primary partition
(hd0,2)   third primary partition
(hd0,3)   fourth primary partition (usually an extended partition)
(hd0,4)   first logical partition
(hd0,5)   second logical partition
```

Sendo dependente de dispositivos BIOS, o GRUB não faz distinção entre dispositivos PATA (IDE), SATA, SCSI e RAID de hardware. Todos os discos rígidos reconhecidos pelo BIOS ou por outras controladoras são numerados de acordo com a sequência de boot predefinido no BIOS.

Infelizmente, geralmente não é possível mapear os nomes dos dispositivos Linux de forma exata para os nomes dos dispositivos BIOS. Ele gera esse mapeamento com a ajuda de um algoritmo e o grava no arquivo device.map, que pode ser editado se necessário. Na Seção 12.1.2, “O arquivo device.map” (p 151), há informações sobre o arquivo device.map.

O caminho completo do GRUB consiste em um nome de dispositivo escrito entre parênteses e no caminho para o arquivo no sistema de arquivos na partição especificada. O caminho começa com uma barra. Por exemplo, o kernel inicializável pode ser especificado como a seguir em um sistema com um único disco rígido PATA (IDE) com o Linux em sua primeira partição:

```
(hd0,0)/boot/vmlinuz
```

12.1.1.2 Um exemplo de arquivo de menu

O exemplo a seguir mostra a estrutura de um arquivo de menu do GRUB. A instalação de exemplo compreende uma partição de boot do Linux em `/dev/sda5`, uma partição raiz em `/dev/sda7` e uma instalação do Windows em `/dev/sda1`.

```
gfxmenu (hd0,4)/boot/message❶
color white/blue black/light-gray❷
default 0❸
timeout 8❹

title linux❺
   root (hd0,4)
   kernel /boot/vmlinuz root=/dev/sda7 vga=791 resume=/dev/sda9
   initrd /boot/initrd

title windows❻
   rootnoverify (hd0,0)
   chainloader +1

title floppy❼
   rootnoverify (hd0,0)
   chainloader (fd0)+1

title failsafe❽
   root (hd0,4)
   kernel /boot/vmlinuz.shipped root=/dev/sda7 ide=nodma \
   apm=off acpi=off vga=normal nosmp maxcpus=0 3 noresume
   initrd /boot/initrd.shipped
```

O primeiro bloco define a configuração da splash screen:

❶ A imagem de fundo `message` localiza-se no diretório `/boot` da partição `/dev/sda5`.

❷ Esquema de cores: branco (primeiro plano), azul (segundo plano), preto (seleção) e cinza claro (segundo plano da seleção). O esquema de cores não tem efeito sobre a tela de apresentação, apenas sobre o menu personalizável do GRUB que você pode acessar saindo da tela de apresentação com Esc.

❸ A primeira (`0`) entrada do menu `title linux` é inicializada por padrão.

❹ Após oito segundos sem nenhuma entrada do usuário, o GRUB inicializa automaticamente a entrada default. Para desativar o boot automático, apague a linha `timeout`. Se você definir `timeout 0`, o GRUB inicializa a entrada default imediatamente.

O segundo e maior bloco lista os vários sistemas operacionais inicializáveis. As seções para os sistemas operacionais individuais são introduzidas pelo `título`.

❺ A primeira entrada (`title linux`) é responsável por inicializar o SUSE Linux Enterprise Desktop. O kernel (`vmlinuz`) localiza-se na primeira partição lógica (a partição de boot) do primeiro disco rígido. Os parâmetros do kernel, tais como a partição raiz e o modo VGA, são anexados aqui. A partição raiz é especificada de acordo com a convenção de nomeação do Linux (`/dev/sda7/`), pois essas informações são lidas pelo kernel e não têm nenhuma relação com o GRUB. O `initrd` também se localiza na primeira partição lógica do primeiro disco rígido.

❻ A segunda entrada é responsável por carregar o Windows. O Windows é inicializado a partir da primeira partição do primeiro disco rígido (`hd0,0`). O comando `chainloader +1` faz com que o GRUB leia e execute o primeiro setor da partição especificada.

❼ A próxima entrada permite o boot a partir do disco rígido sem modificar as configurações do BIOS.

❽ A opção de boot `failsafe` inicia o Linux com uma seleção de parâmetros do kernel que permite que o Linux seja inicializado nos sistemas problemáticos.

O arquivo de menu pode ser mudado sempre que for necessário. O GRUB utiliza, então, as configurações modificadas durante o próximo boot. Edite o arquivo permanentemente usando o YaST ou um editor da sua escolha. Como alternativa, faça as alterações temporárias de forma interativa usando a função de edição do GRUB. Consulte o Seção 12.1.1.3, “Editando as entradas de menu durante o procedimento de boot” (p 150).

12.1.1.3 Editando as entradas de menu durante o procedimento de boot

No menu gráfico de boot, selecione o sistema operacional a ser inicializado com as teclas de seta. Se selecionar um sistema Linux, você pode inserir parâmetros extras de boot no prompt de boot. Para editar diretamente as entradas individuais do menu, pressione Esc para sair da tela de apresentação e entrar no menu baseado em texto do GRUB e depois pressione E. As mudanças feitas desta maneira só se aplicam ao boot atual, não sendo adotadas permanentemente.

IMPORTANTE: layout do teclado durante o procedimento de boot

O layout do teclado norte-americano é o único disponível na hora de inicializar. Consulte a Figura 31.3, "Layout do teclado dos EUA" (p 445).

Editar entradas de menu facilita o reparo de um sistema com defeito que não pode mais ser inicializado, pois o arquivo de configuração defeituoso do carregador de boot pode ser evitado ao se inserir parâmetros manualmente. A inserção manual de parâmetros durante o procedimento de boot também é útil para testar novas configurações sem danificar o sistema nativo.

Depois de ativar o modo de edição, use as teclas de seta para selecionar a entrada de menu cuja configuração deve ser editada. Para tornar a configuração editável, pressione E novamente. Dessa maneira, edite as especificações incorretas das partições ou do caminho antes que tenham um efeito negativo sobre o processo de boot. Pressione Enter para sair do modo de edição e retornar ao menu. Depois pressione B para inicializar essa entrada. No texto de ajuda da parte inferior, são mostradas mais ações possíveis.

Para inserir permanentemente as opções de boot mudadas e passá-las para o kernel, abra o arquivo `menu.lst` como usuário `root` e anexe os respectivos parâmetros do kernel à linha existente, separados por espaços:

```
title linux
   root(hd0,0)
     kernel /vmlinuz root=/dev/sda3 additional parameter
   initrd /initrd
```

O GRUB adota automaticamente os novos parâmetros na próxima vez em que o sistema é inicializado. Como alternativa, essa alteração também pode ser feita com o módulo do carregador de boot YaST. Anexe os novos parâmetros à linha existente, separados por espaços.

12.1.2 O arquivo device.map

O arquivo `device.map` mapeia os nomes de dispositivos do GRUB e do BIOS para os nomes de dispositivos do Linux. Em um sistema misto que contém discos rígidos PATA (IDE) e SCSI, o GRUB deve tentar determinar a sequência de boot por meio de um procedimento especial, pois talvez ele não tenha acesso às informações do BIOS na sequência de boot. O GRUB salva o resultado desta análise no arquivo `/boot/grub/device.map`. Arquivos `device.map` de exemplo para um sistema no qual

a sequência de boot no BIOS é definida como PATA antes de SCSI podem ser parecidos com o seguinte:

```
(fd0)  /dev/fd0
(hd0)  /dev/sda
(hd1)  /dev/sdb
```

ou

```
(fd0)  /dev/fd0
(hd0)  /dev/disk-by-id/DISK1 ID
(hd1)  /dev/disk-by-id/DISK2 ID
```

Como a ordem de discos rígidos PATA (IDE), SCSI e outros depende de vários fatores, e como o Linux não consegue identificar o mapeamento, a sequência no arquivo `device.map` pode ser definida manualmente. Se você encontrar problemas durante a inicialização, verifique se a sequência neste arquivo corresponde à sequência no BIOS e use o prompt do GRUB para modificá-la temporariamente, se necessário. Depois que o sistema Linux for inicializado, o arquivo `device.map` pode ser permanentemente editado com o módulo do carregador de boot YaST ou com um editor da sua preferência.

Depois de alterar manualmente o `device.map`, execute o seguinte comando para reinstalar o GRUB. Este comando faz com que o arquivo `device.map` seja recarregado e os comandos listados em `grub.conf` sejam executados:

```
grub --batch < /etc/grub.conf
```

12.1.3 O arquivo /etc/grub.conf

O terceiro arquivo de configuração importante do GRUB, depois do `menu.lst` e do `device.map`, é o `/etc/grub.conf`. Esse arquivo contém os comandos, os parâmetros e as opções que o shell do GRUB precisa para instalar corretamente o carregador de boot:

```
setup --stage2=/boot/grub/stage2 --force-lba (hd0,1) (hd0,1)
   quit
```

Esse comando instrui o GRUB a instalar automaticamente o carregador de boot na segunda partição do primeiro disco rígido (hd0,1) usando as imagens de boot localizadas na mesma partição. O parâmetro `--stage2=/boot/grub/stage2` é necessário para instalar a imagem `stage2` de um sistema de arquivos montado. Alguns BIOS possuem falha na implementação do suporte a LBA. `--force-lba` proporciona uma solução para ignorá-la.

12.1.4 O arquivo /etc/sysconfig/bootloader

Esse arquivo de configuração só é usado para configurar o carregador de boot com o YaST e sempre que um novo kernel é instalado. Ele é avaliado pela biblioteca perl-bootloader, que modifica o arquivo de configuração do carregador de boot de acordo (por exemplo, `/boot/grub/menu.lst` para o GRUB). O `/etc/sysconfig/bootloader` não é um arquivo de configuração específico do GRUB, os valores são aplicados a qualquer carregador de boot instalado no SUSE Linux Enterprise Desktop.

NOTA: Configuração do carregador de boot após atualização do kernel

Sempre que um novo kernel é instalado, o perl-bootloader grava um novo arquivo de configuração do carregador de boot (por exemplo, `/boot/grub/menu.lst` para o GRUB) usando os padrões especificados em `/etc/sysconfig/bootloader`. Se você estiver usando um conjunto personalizado de parâmetros de kernel, certifique-se de ajustar os padrões relevantes em `/etc/sysconfig/bootloader` de acordo com as suas necessidades.

`LOADER_TYPE`
: Especifica o carregador de boot instalado no sistema (ex. GRUB ou LILO). Não modifique, use o YaST para mudar o carregador de boot, conforme descrito em Procedimento 12.6, “Mudando o tipo de carregador de boot” (p 161).

`DEFAULT_VGA/FAILSAFE_VGA / XEN_VGA`
: A resolução de tela e a profundidade de cores do buffer de quadros usadas durante o boot são configuradas com o parâmetro de kernel `vga`. Esses valores definem qual resolução e profundidade de cores usar para as entradas de boot default, failsafe e XEN. Os seguintes valores são válidos:

***Tabela 12.1** Referência de resolução de tela e profundidade de cores*

	640x480	**800x600**	**1024 x 768**	**1280x1024**	**1600x1200**
8bit	0x301	0x303	0x305	0x307	0x31C
15bit	0x310	0x313	0x316	0x319	0x31D
16bit	0x311	0x314	0x317	0x31A	0x31E

	640x480	800x600	1024 x 768	1280x1024	1600x1200
24bit	0x312	0x315	0x318	0x31B	0x31F

`DEFAULT_APPEND/FAILSAFE_APPEND/XEN_KERNEL_APPEND`
: Parâmetros do kernel (diferentes do `vga`) que são automaticamente anexados às entradas de boot padrão, de failsafe e do XEN no arquivo de configuração do carregador de boot.

`CYCLE_DETECTION/CYCLE_NEXT_ENTRY`
: Configure se deseja usar a detecção do ciclo de boot e, em caso afirmativo, qual entrada alternativa de `/boot/grub/menu.lst` usar no boot em caso de um ciclo de reinicialização (por exemplo, `Failsafe`). Consulte `/usr/share/doc/packages/bootcycle/README` para obter informações detalhadas.

12.1.5 Configurando uma senha de boot

Mesmo antes da inicialização do sistema operacional, o GRUB permite acesso aos sistemas de arquivos. Os usuários que não têm permissões raiz podem acessar os arquivos no seu sistema Linux aos quais não têm acesso depois que o sistema é inicializado. Para bloquear esse tipo de acesso ou impedir que os usuários inicializem certos sistemas operacionais, defina uma senha de boot.

IMPORTANTE: senha de boot e splash screen

Se você usar uma senha de boot para o GRUB, a tela normal de apresentação não será exibida.

Como o usuário `root`, proceda da seguinte forma para definir uma senha de boot:

1 No prompt do root, criptografe a senha usando grub-md5-crypt:

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

2 Cole a string criptografada na seção global do arquivo `menu.lst`:

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

Agora os comandos do GRUB só podem ser executados no prompt raiz depois que se pressionar P e se inserir a senha. No entanto, os usuários ainda podem inicializar todos os sistemas operacionais a partir do menu de boot.

3 Para impedir que um ou vários sistemas operacionais sejam inicializados a partir do menu de boot, acrescente a entrada `lock` em cada seção no `menu.lst` que não deveria ser inicializada sem se inserir uma senha. Por exemplo:

```
title linux
   kernel (hd0,4)/vmlinuz root=/dev/sda7 vga=791
   initrd (hd0,4)/initrd
   lock
```

Depois de reiniciar o sistema e selecionar a entrada no Linux no menu de boot, é exibida a seguinte mensagem de erro:

```
Error 32: Must be authenticated
```

Pressione Enter para inserir o menu. Depois pressione P para obter o prompt da senha. Depois de inserir a senha e pressionar Enter, o sistema operacional selecionado (o Linux, neste caso) não deve inicializar.

12.2 Configurando o carregador de boot com o YaST

O modo mais fácil de configurar o carregador de boot em seu sistema SUSE Linux Enterprise Desktop é utilizar o módulo do YaST. No Centro de Controle do YaST, selecione *Sistema* > *Carregador de Boot*. Como na Figura 12.1, “Configurações do carregador de boot” (p 156), isso mostra a configuração do carregador de boot atual do sistema e permite fazer mudanças.

Figura 12.1 Configurações do carregador de boot

Use a guia *Gerenciamento de Seções* para editar, mudar e apagar seções do carregador de boot referentes aos sistemas operacionais individuais. Para adicionar uma opção, clique em *Adicionar*. Para mudar o valor de uma opção existente, selecione-o com o mouse e clique em *Editar*. Para remover uma entrada existente, selecione-a e clique em *Apagar*. Se não estiver familiarizado com as opções do carregador de boot, leia primeiro a Seção 12.1, "Inicializando com o GRUB" (p 144).

Use a guia *Instalação do Carregador de Boot* para ver e mudar configurações relativas a tipo, local e opções avançadas do carregador.

Clique em *Outros* para acessar as opções de configurações avançadas. O editor incorporado permite mudar os arquivos de configuração do GRUB. Para obter os detalhes, consulte a Seção 12.1, "Inicializando com o GRUB" (p 144). Você também pode apagar a configuração existente e *Iniciar*, ou deixar o YaST *Propor Nova Configuração*. Também é possível gravar a configuração em disco ou relê-la do disco. Para restaurar o MBR (Master Boot Record) original que foi gravado durante a instalação, escolha *Recuperar MBR do Disco Rígido*.

12.2.1 Ajustando a entrada de boot padrão

Para mudar o sistema que é inicializado por padrão, proceda da seguinte maneira:

Procedimento 12.1 *Definindo o sistema padrão*

1 Abra a guia *Gerenciamento de Seções*.

2 Selecione a entrada desejada na lista.

3 Clique em *Definir como Padrão*.

4 Clique em *OK* para ativar essas mudanças.

12.2.2 Modificando a localização do carregador de boot

Para modificar o local do carregador de boot, siga estas etapas:

Procedimento 12.2 *Mudando a localização do carregador de boot*

1 Selecione a guia *Instalação do Carregador de Boot* e escolha uma das seguintes opções para a *Localização do Carregador de Boot*:

Boot do Master Boot Record
Instala o carregador de boot no MBR do primeiro disco (de acordo com a sequência de boot predefinida no BIOS).

Boot da partição raiz
Instala o carregador de boot no setor de boot da partição `/` (padrão).

Boot da partição de boot
Instala o carregador de boot no setor de boot da partição `/boot`.

Boot da partição estendida
Instala o carregador de boot no container da partição estendida.

Partição de boot personalizada
Use esta opção para especificar a localização do carregador de boot manualmente.

2 Clique em *OK* para aplicar as mudanças.

12.2.3 Mudando o tempo de espera do carregador de boot

O carregador de boot não inicializa o sistema padrão imediatamente. Durante o tempo de espera, você pode selecionar o sistema para inicializar ou gravar alguns parâmetros de kernel. Para definir o tempo de espera do carregador de boot, proceda da seguinte maneira:

Procedimento 12.3 *Mudando o tempo de espera do carregador de boot*

1 Abra a guia *Instalação do Carregador de Boot*.

2 Clique em *Opções do Carregador de Boot*.

3 Mude o valor de *Tempo de Espera em Segundos* digitando um novo valor e clicando na tecla de seta adequada com o mouse ou usando as teclas de seta do teclado.

4 Clique em *OK* duas vezes para gravar as mudanças.

ATENÇÃO: Tempo de espera de 0 segundos

Ao definir o tempo de espera como 0 segundo, não será possível acessar o GRUB durante o tempo de boot. Quando tiver definido a opção de boot padrão para um sistema operacional não Linux ao mesmo tempo, isso efetivamente desabilitará o acesso ao sistema Linux.

12.2.4 Configurando uma senha de boot

Utilizando este módulo do YaST, é possível definir uma senha para proteger a inicialização. Este procedimento aumenta o nível de segurança.

Procedimento 12.4 *Configurando uma senha do carregador de boot*

1 Abra a guia *Instalação do Carregador de Boot*.

2 Clique em *Opções do Carregador de Boot*.

3. Ative a opção *Proteger Carregador de Boot com Senha* com um clique e digite a sua *Senha* duas vezes.

4. Clique em *OK* duas vezes para gravar as mudanças.

12.2.5 Ajustando a ordem dos discos

Se o seu computador tiver mais de um disco rígido, é possível especificar a sequência de boot dos discos para corresponder à configuração do BIOS da máquina (consulte a Seção 12.1.2, “O arquivo device.map” (p 151)). Para fazer isso, proceda da seguinte maneira:

Procedimento 12.5 *Definindo a ordem dos discos*

1. Abra a guia *Instalação do Carregador de Boot*.

2. Clique em *Detalhes de Instalação do Carregador de Boot*.

3. Se mais de um disco for listado, selecione um disco e clique em *Para cima* ou *Para baixo* para reordenar os discos exibidos.

4. Clique em *OK* duas vezes para gravar as mudanças.

12.2.6 Configurando as opções avançadas

As opções avançadas de boot podem ser configuradas por meio de *Instalação do Carregador de Boot* > *Opções do Carregador de Boot*. Normalmente não há necessidade de mudar as configurações padrão.

Definir Flag Ativo na Tabela de Partição para a Partição de Boot
: Ativa a partição que contém o carregador de boot. Alguns sistemas operacionais legados (como o Windows 98) podem ser inicializados apenas de uma partição ativa.

Gravar Código de Boot Genérico no MBR
: Substitui o MBR atual por um código genérico independente de sistema operacional.

Flag de Depuração
Define o GRUB no modo de depuração, no qual são exibidas mensagens para mostrar a atividade do disco.

Ocultar Menu de Boot
Oculta o menu de boot e a entrada padrão.

ATENÇÃO

Ao ocultar o menu de boot, não será possível acessar o GRUB durante o tempo de boot. Quando tiver definido a opção de boot padrão para um sistema operacional não Linux ao mesmo tempo, isso efetivamente desabilitará o acesso ao sistema Linux.

Usar GRUB Confiável
Inicia o GRUB Confiável, que suporta a funcionalidade de computação confiável.

Arquivo de Menu Gráfico
Caminho do arquivo gráfico usado na exibição da tela de boot.

Parâmetros de Conexão Serial
Se a sua máquina é controlada por um console serial, você pode especificar a porta COM que será usada e em qual velocidade. Além disso, defina *Definição de Terminal* como “serial”. Consulte `info grub` ou `http://www.gnu.org/software/grub/manual/grub.html` para obter os detalhes.

Usar o Console Serial
Se a sua máquina é controlada por um console serial, ative essa opção e especifique a porta COM que será usada e em qual velocidade. Consulte `info grub` ou o site `http://www.gnu.org/software/grub/manual/grub.html#Serial-terminal`

12.2.7 Mudando o tipo de carregador de boot

Defina o tipo de carregador de boot em *Instalação do Carregador de Boot*. O carregador de boot padrão no SUSE Linux Enterprise Desktop é o GRUB. Para usar o LILO ou o ELILO, proceda da seguinte maneira:

ATENÇÃO: O LILO não é suportado

Não é recomendado usar o LILO, ele não é suportado no SUSE Linux Enterprise Desktop. Use-o apenas em casos especiais.

Procedimento 12.6 *Mudando o tipo de carregador de boot*

1. Selecione a guia *Instalação do Carregador de Boot*.

2. Para *Carregador de Boot*, selecione *LILO*.

3. Na caixa de diálogo aberta, selecione uma das seguintes ações:

   Propor Nova Configuração
   : Faça com que o YaST proponha uma nova configuração.

   Converter Configuração Atual
   : Faça com que o YaST converta a configuração atual. Na conversão da configuração, algumas definições podem ser perdidas.

   Iniciar Nova Configuração do Início
   : Grave uma configuração personalizada. Esta ação não está disponível durante a instalação do SUSE Linux Enterprise Desktop.

   Ler Configuração Gravada em Disco
   : Carregue o `/etc/lilo.conf`. Esta ação não está disponível durante a instalação do SUSE Linux Enterprise Desktop.

4. Clique em *OK* duas vezes para gravar as mudanças.

Durante a conversão, a antiga configuração do GRUB é gravada no disco. Para usá-la, basta voltar o tipo de carregador de boot para GRUB e escolher *Recuperar Configuração Salva antes da Conversão*. Esta ação fica disponível somente em um sistema instalado.

NOTA: carregador de boot personalizado

Para usar um carregador de boot que não seja o GRUB nem o LILO, selecione *Não instalar nenhum carregador de boot*. Leia a documentação do seu carregador de boot cuidadosamente antes de escolher esta opção.

12.3 Desinstalando a controladora de boot do Linux

O YaST pode ser usado para desinstalar o carregador de boot do Linux e recuperar o MBR para o estado que ele tinha antes da instalação do Linux. Durante a instalação, o YaST cria automaticamente uma cópia de backup do MBR original e a restaura mediante solicitação.

Para desinstalar o GRUB, inicie o YaST e clique em *Sistema* > *Carregador de Boot* para iniciar o módulo do carregador de boot. Selecione *Outro* > *Recuperar MBR do Disco Rígido* e confirme com *Sim, Regravar*.

12.4 Criando CDs de boot

Se o boot do sistema com um gerenciador de boot apresentar problemas ou se o gerenciador de boot não puder ser instalado no disco rígido, também será possível criar um CD inicializável com todos os arquivos de inicialização necessários para o Linux. Para isso, é necessário um gravador de CD instalado no sistema.

A criação de um CR-ROM inicializável com GRUB requer simplesmente um formato especial de *stage2* chamado`stage2_eltorito` e, opcionalmente, um `menu.lst` personalizado. Os clássicos arquivos `stage1` e `stage2` não são necessários.

Procedimento 12.7 *Criando CDs de boot*

1 Passe para um diretório no qual será criada a imagem ISO, por exemplo: `cd /tmp`

2 Crie um subdiretório para o GRUB e mude para o diretório `iso` recém-criado:

```
mkdir -p iso/boot/grub && cd iso
```

3 Copie o kernel, os arquivos `stage2_eltorito`, `initrd`, `menu.lst` e `message` para `iso/boot/`:

```
cp /boot/vmlinuz boot/
cp /boot/initrd boot/
cp /boot/message boot/
cp /usr/lib/grub/stage2_eltorito boot/grub
cp /boot/grub/menu.lst boot/grub
```

Em alguns casos (ao inicializar vários sistemas operacionais, por exemplo), também pode ser útil copiar `/boot/grub/device.map` para `boot/grub`.

4. Substitua as entradas `root (hdx, y)` por `root (cd)` para apontar para o dispositivo de CD_ROM. Você também pode ter que ajustar os caminhos para o arquivo de mensagem, o kernel e o initrd — eles devem apontar para `/boot/message`, `/boot/vmlinuz` e `/boot/initrd`, respectivamente. Depois de fazer os ajustes, `menu.lst` deverá ter aparência semelhante ao exemplo a seguir:

```
timeout 8
default 0
gfxmenu (cd)/boot/message

title Linux
   root (cd)
   kernel /boot/vmlinuz root=/dev/sda5 vga=794 resume=/dev/sda1 \
   splash=verbose showopts
   initrd /boot/initrd
```

   Use `splash=silent` em vez de `splash=verbose` para impedir que apareçam mensagens de boot durante o procedimento de boot.

5. Crie a imagem ISO com o seguinte comando:

```
genisoimage -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -iso-level 2 -input-charset utf-8 \
-o grub.iso /tmp/iso
```

6. Grave o arquivo resultante `grub.iso` em um CD usando seu utilitário preferido. Não grave a imagem ISO como arquivo de dados, porém, use a opção para gravar uma imagem de CD no seu utilitário de gravação.

12.5 A tela gráfica do SUSE

A tela gráfica do SUSE será exibida no primeiro console se a opção `vga=valor` for usada como parâmetro de kernel. Se você fizer a instalação usando o YaST, essa opção é automaticamente ativada de acordo com a resolução e a placa de vídeo selecionadas. Há três maneiras de desativar a tela SUSE, se desejado:

Desabilitando a tela do SUSE quando necessário
: Insira o comando `echo 0 >/proc/splash` na linha de comando para desativar a tela gráfica. Para ativá-la novamente, insira `echo 1 >/proc/splash`.

Desabilitando a tela do SUSE por padrão.
: Acrescente o parâmetro de kernel `splash=0` à configuração do seu carregador de boot. O Capítulo 12, *O carregador de boot GRUB* (p 143) fornece mais informações sobre isso. No entanto, se você preferir o modo de texto (que foi o padrão nas versões anteriores), defina `vga=normal`.

Desativando completamente a tela SUSE
: Compile um novo kernel e desative a opção *Usar a splash screen em vez do logotipo de boot* no suporte a framebuffer. A desabilitação do suporte a buffer de quadros no kernel também desabilita automaticamente a splash screen.

ATENÇÃO: Sem suporte

O SUSE não pode fornecer suporte ao seu sistema se você o executar com um kernel personalizado.

12.6 Solução de problemas

Essa seção lista alguns dos problemas frequentemente encontrados na hora de inicializar com o GRUB e uma breve descrição das possíveis soluções. Alguns desses problemas são abordados em artigos da Base de Dados de Conhecimento, em `http://www.suse.com/support`. Use a caixa de diálogo de pesquisa para procurar palavras-chave como *GRUB*, *boot* e *carregador de boot*.

GRUB e XFS
: O XFS não deixa espaço para o `stage1` no bloco de boot da partição. Portanto, não especifique uma partição XFS como local do carregador de boot. Esse problema pode ser resolvido com a criação de uma partição separada de boot que não é formatada com o XFS.

O GRUB relata um erro de geometria no GRUB
: O GRUB verifica a geometria dos discos rígidos conectados quando o sistema é inicializado. Às vezes, a BIOS retorna informações inconsistentes e o GRUB cria um erro de geometria do GRUB. Quando isso ocorrer, atualize o BIOS.

  O GRUB também retorna essa mensagem de erro se o Linux foi instalado em um disco rígido adicional não registrado no BIOS. O *stage1* do carregador de boot foi

encontrado e carregado corretamente, mas o *stage2* não foi encontrado. Esse problema pode ser remediado registrando-se o novo disco rígido no BIOS.

Sistema contendo vários discos rígidos não é inicializado
: Durante a instalação, o YaST talvez tenha determinado incorretamente a sequência de boot dos discos rígidos. Por exemplo, o GRUB pode considerar o disco PATA (IDE) como `hd0` e o disco SCSI como `hd1`, embora a sequência de boot no BIOS seja invertida (SCSI *antes de* PATA).

  Nesse caso, corrija os discos rígidos durante o processo de boot com a ajuda da linha de comando do GRUB. Depois que o sistema for inicializado, edite `device.map` para aplicar o novo mapeamento permanentemente. Depois verifique os nomes de dispositivo do GRUB nos arquivos `/boot/grub/menu.lst` e `/boot/grub/device.map` e reinstale o carregador de boot com o seguinte comando:

```
grub --batch < /etc/grub.conf
```

Inicializando o Windows do segundo disco rígido
: Alguns sistemas operacionais, como o Windows, podem ser inicializados apenas do primeiro disco rígido. Se um sistema operacional desse tipo for instalado em um disco rígido que não for o primeiro, você pode efetuar uma mudança lógica na respectiva entrada do menu.

```
...
title windows
   map (hd0) (hd1)
   map (hd1) (hd0)
   chainloader(hd1,0)+1
...
```

  Nesse exemplo, o Windows é iniciado a partir do segundo disco rígido. Para essa finalidade, a ordem lógica dos discos rígidos é mudada com `map`. Essa alteração não afeta a lógica dentro do arquivo de menu do GRUB. Portanto, o segundo disco rígido deve ser especificado para `chainloader`.

12.7 Para obter mais informações

Em `http://www.gnu.org/software/grub/`, há informações abrangentes sobre o GRUB Consulte também a página de informações `grub`. Você também pode

pesquisar a palavra-chave “GRUB ” na Pesquisa de Informações Técnicas em http://www.novell.com/support para obter informações sobre problemas específicos.

UEFI (Unified Extensible Firmware Interface) 13

UEFI (Unified Extensible Firmware Interface) é a interface entre o firmware que vem com o hardware do sistema, todos os componentes do hardware do sistema e o sistema operacional.

A UEFI está se tornando cada vez mais disponível em sistemas PC e substituindo o PC-BIOS tradicional. Por exemplo, a UEFI suporta apropriadamente sistemas de 64 bits e oferece inicialização segura ("Boot Seguro", firmware versão 2.3.1c ou superior necessário), que é um dos recursos mais importantes. Por último mas não menos importante, com a UEFI, um firmware padrão torna-se disponível em todas as plataformas x86.

A UEFI oferece também as seguintes vantagens:

- Inicialização de discos grandes (mais de 2 TiB) com GPT (Tabela de Partição GUID).
- Drivers e arquitetura independente da CPU.
- Ambiente pré-OS flexível com recursos de rede.
- CSM (Módulo de Suporte de Compatibilidade) para suportar inicialização de sistemas operacionais legados por emulação do tipo PC-BIOS.

Para obter mais informações, consulte http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface. As seguintes seções não são uma visão geral da UEFI, são apenas dicas sobre como alguns recursos são implementados no SUSE Linux Enterprise.

13.1 Boot seguro

Para a UEFI, proteger o processo de boot significa estabelecer uma cadeia de confiança. A “plataforma” é a raiz da cadeia de confiança; no contexto do SUSE Linux Enterprise, a placa-mãe e o firmware on-board podem ser considerados a “plataforma”. Explicando de uma maneira um pouco diferente, imagine o fornecedor do hardware e a cadeia de confiança que parte desse fornecedor para os fabricantes dos componentes, os fornecedores de OS, etc.

A confiança é expressada através da criptografia de chave pública. O fornecedor do hardware coloca a chamada PK (Chave de Plataforma) no firmware, representando a base da confiança. A relação de confiança com os fornecedores do sistema operacional e os outros é documentada pela assinatura das chaves usando a Chave de Plataforma.

Por fim, a segurança é estabelecida exigindo que nenhum código seja executado pelo firmware, exceto se tiver sido assinado por uma das chaves “confiáveis”, seja um carregador de boot de OS, algum driver localizado na memória flash de uma placa PCI Express ou no disco, seja uma atualização do próprio firmware.

Basicamente, para usar o Boot Seguro, o carregador de OS deve ser assinado com uma chave de confiança do firmware, e você precisa que o carregador de OS verifique se o kernel que ele carrega pode ser confiado.

É possível adicionar Chaves de Troca de Chave (KEK) ao banco de dados de chaves UEFI. Dessa forma, é possível usar outros certificados, desde que sejam assinados com a parte privada da PK.

13.1.1 Implementação no SUSE Linux Enterprise

A Chave de Troca de Chave (KEK) da Microsoft é instalada por padrão.

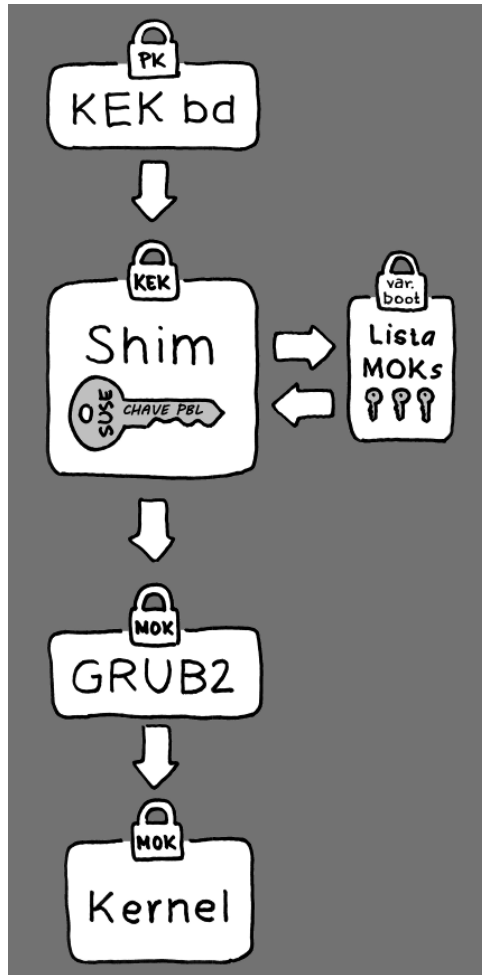
NOTA: GPT (Tabela de Partição GUID) obrigatória

O recurso Boot Seguro requer que a GPT (Tabela de Partição GUID) substitua o particionamento antigo por um MBR (Master Boot Record).

Se o YaST detectar o modo EFI durante a instalação, ele tentará criar uma partição GPT. A UEFI espera encontrar os programas EFI na ESP (Partição de Sistema EFI) formatada por FAT.

O suporte a Boot Seguro UEFI requer basicamente um carregador de boot com assinatura digital que o firmware reconheça como uma chave confiável. Para ser útil aos clientes do SUSE Linux Enterprise, a chave precisa ser, antes de tudo, de confiança do firmware, sem exigir intervenção manual.

Há duas formas de conseguir isso. Uma é trabalhar com os fornecedores do hardware para que eles endossem uma chave do SUSE, que o SUSE usará para assinar o carregador de boot. A outra é utilizar o programa de Certificação de Logotipo do Windows da Microsoft para certificar o carregador de boot e para a Microsoft reconhecer a chave de assinatura do SUSE (isto é, assiná-lo com sua KEK). Até agora, o SUSE assinava o carregador pelo Serviço de Assinatura UEFI (que é a Microsoft, neste caso).

Figura 13.1 UEFI: processo de boot seguro

Na camada de implementação, o SUSE usa o carregador `shim`, uma solução inteligente que evita problemas legais e simplifica a etapa de certificação e assinatura consideravelmente. A tarefa do carregador `shim` é carregar um carregador de boot, como eLILO ou GRUB 2 e verificá-lo; e o carregador de boot, em troca, carrega os kernels assinados apenas por uma chave do SUSE. O SUSE oferece essa funcionalidade com o SLE11 SP3 em instalações novas que tenham o Boot Seguro UEFI habilitado.

Há dois tipos de usuários confiáveis:

- Primeiro, os que detêm as chaves. A Chave de Plataforma (PK) permite quase tudo. A Chave de Troca de Chave (KEK) permite tudo o que pode uma PK, exceto modificar a PK.

- Segundo, qualquer pessoa com acesso físico à máquina. Um usuário com acesso físico pode reinicializar a máquina e configurar a UEFI.

A UEFI oferece dois tipos de variáveis para atender às necessidades desses usuários:

- A primeira são as chamadas “Variáveis Autenticadas”, que podem ser atualizadas tanto do processo de boot (o chamado Ambiente de Serviços de Boot) quanto do OS em execução, mas apenas quando o novo valor da variável é assinado com a mesma chave que assinou o valor antigo da variável. E elas só podem ser anexadas ou modificadas para um valor com número de série maior.

- A segunda são as chamadas “Variáveis Apenas de Serviços de Boot”. Essas variáveis estão acessíveis a qualquer código executado durante o processo de boot. Após o término do processo de boot e antes de iniciar o OS, o carregador de boot deve chamar `ExitBootServices`. Depois disso, essas variáveis não estarão mais acessíveis, e o OS não poderá usá-las.

As várias listas de chaves UEFI são do primeiro tipo, já que permitem atualização online, adição e lista negra de chaves, drivers e impressões digitais do firmware. É o segundo tipo de variável, a “Variável Apenas de Serviços de Boot”, que ajuda a implementar o Boot Seguro de forma segura, pronta para código-fonte aberto e também compatível com GPLv3.

O SUSE começa com o `shim`, um carregador de boot EFI pequeno e simples, que foi originalmente desenvolvido pela Fedora. Ele é assinado por um certificado assinado pela KEK do SUSE e um certificado emitido pela Microsoft, com base nas KEKs disponíveis no banco de dados de chaves UEFI do sistema.

Dessa forma, o `shim` pode ser carregado e executado.

O `shim` continua para verificar se o carregador de boot que deseja carregar é confiável. Em uma situação padrão, o `shim` usa um certificado do SUSE independente incorporado. Além disso, o `shim` permite “inscrever” outras chaves, anulando a chave padrão do SUSE. A seguir, nós as chamamos de “Chaves do Proprietário da Máquina” ou MOKs, para abreviar.

Em seguida, o carregador de boot verifica e inicializa o kernel, e o kernel faz o mesmo com os módulos.

13.1.2 MOK (Chave do Proprietário da Máquina)

Se o usuário ("proprietário da máquina") deseja substituir algum componente do processo de boot, as Chaves do Proprietário da Máquina (MOKs) deverão ser usadas. A ferramenta `mokutils` ajuda com a assinatura dos componentes e o gerenciamento das MOKs.

O processo de inscrição começa com a reinicialização da máquina e a interrupção do processo de boot (ex., pressionando uma tecla) quando o `shim` é carregado. O `shim` entra no modo de inscrição, permitindo ao usuário substituir a chave padrão do SUSE pelas chaves de um arquivo na partição de boot. Se o usuário quiser, o `shim` calculará um hash desse arquivo e colocará o resultado em uma variável "Apenas de Serviços de Boot". Dessa forma, o `shim` pode detectar qualquer mudança no arquivo feita fora dos Serviços de Boot e evitar assim uma violação da lista de MOKs aprovadas pelo usuário.

Tudo isso acontece durante a inicialização, apenas o código verificado é executado agora. Portanto, apenas um usuário presente no console pode utilizar o conjunto de chaves do proprietário da máquina. Não é possível que seja um malware ou um invasor com acesso remoto ao OS, pois invasores ou malware só podem mudar o arquivo, mas não o hash armazenado na variável "Apenas de Serviços de Boot".

O carregador de boot, após ser carregado e verificado pelo `shim`, chamará de novo o `shim` para verificar o kernel, evitando a duplicação do código de verificação. O `shim` usa a mesma lista de MOKs para isso e avisa o carregador de boot se ele pode carregar o kernel.

Dessa forma, você pode instalar seu próprio kernel ou carregador de boot. Só é necessário instalar um novo conjunto de chaves e autorizá-las estando fisicamente presente durante a primeira reinicialização. Como as MOKs são uma lista, e não apenas uma única MOK, é possível fazer com que o `shim` confie nas chaves de vários fornecedores diferentes, permitindo dual-boot e multi-boot pelo carregador de boot.

13.1.3 Inicializando um kernel personalizado

As informações a seguir são baseadas no http://en.opensuse.org/openSUSE:UEFI#Booting_a_custom_kernel.

O Boot Seguro não impede você de usar um kernel autocompilado. Você deve apenas assiná-lo com seu próprio certificado e tornar esse certificado reconhecível para o firmware ou a MOK.

1. Crie uma chave X.509 personalizada e um certificado usados para assinatura:

   ```
   openssl req -new -x509 -newkey rsa:2048 -keyout key.asc \
     -out cert.pem -nodes -days 666 -subj "/CN=$USER/"
   ```

   Para obter mais informações sobre como criar certificados, consulte http://en.opensuse.org/openSUSE:UEFI_Image_File_Sign_Tools#Create_Your_Own_Certificate.

2. Empacote a chave e o certificado como uma estrutura PKCS#12:

   ```
   openssl pkcs12 -export -inkey key.asc -in cert.pem \
     -name kernel_cert -out cert.p12
   ```

3. Gere um banco de dados NSS para usar com o comando `pesign`:

   ```
   certutil -d . -N
   ```

4. Importe a chave e o certificado incluídos no PKCS#12 para o banco de dados NSS:

   ```
   pk12util -d . -i cert.p12
   ```

5. “Proteja” o kernel com a nova assinatura usando o comando `pesign`:

   ```
   pesign -n . -c kernel_cert -i arch/x86/boot/bzImage \
     -o vmlinuz.signed -s
   ```

6. Liste as assinaturas na imagem do kernel:

   ```
   pesign -n . -S -i vmlinuz.signed
   ```

   Neste momento, é possível instalar o kernel em `/boot`, como de costume. Como o kernel agora tem uma assinatura personalizada, o certificado usado para a assinatura deve ser importado para o firmware ou a MOK UEFI.

7 Converta o certificado no formato DER para importá-lo para o firmware ou a MOK:

```
openssl x509 -in cert.pem -outform der -out cert.der
```

8 Copie o certificado para o ESP para facilitar o acesso:

```
sudo cp cert.der /boot/efi/
```

9 Use `mokutil` para iniciar a lista de MOKs automaticamente.

Se preferir, este é o procedimento para iniciar a MOK manualmente:

9a Reinicialize

9b No menu do GRUB , pressione a tecla '`c`'.

9c Digite:

```
chainloader $efibootdir/MokManager.efi
boot
```

9d Selecione *Enroll key from disk* (Inscrever chave do disco).

9e Navegue até o arquivo `cert.der` e pressione Enter.

9f Siga as instruções para inscrever a chave. Normalmente, você pressiona '`0`' e '`y`' para confirmar.

Se preferir, o menu do firmware pode oferecer maneiras de adicionar uma nova chave ao Banco de Dados de Assinatura.

13.1.4 Usando drivers que não são de caixa de entrada

Não há suporte para adição de drivers que não são de caixa de entrada (isto é, drivers que não vêm com SLE) após inicialização na instalação com Boot Seguro habilitado. Por padrão, a chave de assinatura usada para SolidDriver/PLDP não é confiável.

No entanto, é possível usar drivers de terceiros durante a instalação com Boot Seguro habilitado de duas formas diferentes:

- Adicionar as chaves necessárias ao banco de dados do firmware usando as ferramentas de gerenciamento do firmware/sistema antes da instalação. Essa opção depende do hardware específico que você usa. Fale com o fornecedor do hardware para obter mais informações.

- Usar uma ISO do driver inicializável em `https://drivers.suse.com/` ou pedir ao fornecedor do hardware para inscrever as chaves necessárias na lista MOK na primeira inicialização.

Para usar a ISO do driver inicializável para inscrever as chaves do driver na lista MOK, siga estas etapas:

1 Grave a imagem ISO em uma mídia de CD/DVD vazia.

2 Inicie a instalação executando boot da nova mídia de CD/DVD, com a mídia do SUSE Linux Enterprise padrão em mãos ou um URL para o servidor de instalação de rede.

Ao fazer uma instalação de rede, digite o URL da fonte de instalação de rede na linha de comando de boot usando a opção `install=`.

Ao instalar de uma mídia ótica, o instalador inicializará primeiro do kit do driver e, em seguida, solicitará para inserir o primeiro disco do produto SUSE Linux Enterprise.

3 Um initrd com os drivers atualizados será usado para instalação.

Para obter mais informações, consulte `https://drivers.suse.com/doc/Usage/Secure_Boot_Certificate.html`.

13.1.5 Limitações

Ao inicializar no modo Boot Seguro, as seguintes restrições se aplicam:

- Imagens ISO hibridificadas não são reconhecidas como inicializáveis nos sistemas UEFI. Dessa forma, a inicialização da UEFI de dispositivos USB não é suportada com o SP3.

- Para que o Boot Seguro não seja facilmente desviado, alguns recursos do kernel são desabilitados durante a execução no modo Boot Seguro.
- Os módulos bootloader e kernel devem ser assinados.
- Kexec e kdump são desabilitados.
- A hibernação (suspensão no disco) é desabilitada.
- O acesso a `/dev/kmem` e `/dev/mem` não é possível, nem mesmo como usuário root.
- O acesso à porta de E/S não é possível, nem mesmo como usuário root. Todos os drivers gráficos X11 devem usar um driver do kernel.
- O acesso a PCI BAR por sysfs não é possível.
- O `custom_method` em ACPI não está disponível.
- Debugfs para o módulo asus-wmi não está disponível.
- O parâmetro `acpi_rsdp` não tem nenhum efeito no kernel.

13.2 Para obter mais informações

- `http://www.uefi.org`: Home page da UEFI onde você encontra as especificações atuais da UEFI.
- Publicações no blog por Olaf Kirch e Vojtěch Pavlík (o capítulo acima é quase todo baseado nessas publicações):
  - `http://www.suse.com/blogs/uefi-secure-boot-plan/`
  - `http://www.suse.com/blogs/uefi-secure-boot-overview/`
  - `http://www.suse.com/blogs/uefi-secure-boot-details/`
- `http://en.opensuse.org/openSUSE:UEFI`: UEFI com openSUSE.

Recursos especiais do sistema 14

Este capítulo começa com informações sobre vários pacotes de software, os consoles virtuais e o layout do teclado. Abordamos componentes de software como `bash`, `cron` e `logrotate`, porque eles foram mudados ou aperfeiçoados durante os últimos ciclos de lançamento. Mesmo que eles sejam pequenos ou considerados de menor importância, talvez os usuários desejem mudar o seu comportamento padrão, porque esses componentes muitas vezes estão intimamente ligados ao sistema. O capítulo termina com uma seção sobre configurações específicas de país e idioma (I18N e L10N).

14.1 Informações sobre pacotes de software especiais

Os programas `bash`, `cron`, `logrotate`, `locate`, `ulimit` e `free` são muito importantes para os administradores de sistema e para muitos usuários. As páginas de manual e de informações são duas fontes úteis de informações sobre comandos, mas as duas nem sempre estão disponíveis. O GNU Emacs é um editor de texto popular e muito configurável.

14.1.1 O pacote bash e /etc/profile

Bash é o shell de sistema padrão. Quando usado com um shell de login, ele lê vários arquivos de inicialização. O Bash os processa na ordem em que são exibidos na lista:

1. /etc/profile
2. ~/.profile
3. /etc/bash.bashrc
4. ~/.bashrc

Faça configurações personalizadas em ~/.profile ou ~/.bashrc. Para assegurar o processamento correto desses arquivos, é necessário copiar as configurações básicas de /etc/skel/.profile ou /etc/skel/.bashrc no diretório pessoal do usuário. É recomendável copiar as configurações de /etc/skel após uma atualização. Execute os seguintes comandos de shell para evitar a perda de ajustes pessoais:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Em seguida, copie os ajustes pessoais novamente dos arquivos *.old.

14.1.2 O pacote cron

Se você deseja executar comandos de maneira regular e automática em segundo plano em horários predefinidos, cron é a ferramenta a ser usada. O cron é orientado por tabelas de horários especialmente formatadas. Alguns deles vêm com o sistema e os usuários poderão criar suas próprias tabelas, se necessário.

As tabelas cron estão localizadas em /var/spool/cron/tabs. /etc/crontab atua como uma tabela cron para todo o sistema. Digite o nome de usuário para executar o comando diretamente após a tabela de tempo e antes do comando. No Exemplo 14.1, “Entrada in /etc/crontab” (p 178), root é digitado. Tabelas específicas de pacote, localizadas em /etc/cron.d, possuem o mesmo formato. Consulte a página de manual do cron (man cron).

Exemplo 14.1 *Entrada in /etc/crontab*

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Você não pode editar /etc/crontab chamando o comando crontab -e. Esse arquivo deve ser carregado diretamente em um editor, modificado e gravado.

Alguns pacotes instalam scripts de shell nos diretórios /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly e /etc/cron.monthly, cuja execução é controlada por /usr/lib/cron/run-crons. /usr/lib/cron/run-crons é executado a cada 15 minutos da tabela principal (/etc/crontab). Isso garante que os processos que tenham sido negligenciados possam ser executados no momento adequado.

Para executar os scripts de manutenção por hora, por dia ou outros scripts de manutenção periódica em horários personalizados, remova os arquivos de marcação de horário regularmente, utilizando as entradas /etc/crontab (consulte o Exemplo 14.2, "/etc/crontab: remova arquivos de marcação de horário" (p 179), que remove a opção por hora antes de cada hora cheia, a opção por dia uma vez ao dia às 2:14, etc.).

Exemplo 14.2 */etc/crontab: remova arquivos de marcação de horário*

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

Se preferir, defina DAILY_TIME em /etc/sysconfig/cron como o horário de início de cron.daily. A configuração de MAX_NOT_RUN assegura que as tarefas diárias sejam acionadas para execução, mesmo se o usuário não ligou o computador no DAILY_TIME especificado por um período mais longo. O valor máximo de MAX_NOT_RUN é 14 dias.

Os trabalhos de manutenção diária de sistema são distribuídos a vários scripts por motivos de clareza. Eles estão contidos no pacote aaa_base. /etc/cron.daily contém, por exemplo, os componentes suse.de-backup-rpmdb, suse.de-clean-tmp ou suse.de-cron-local.

14.1.3 Arquivos de registro: pacote logrotate

Existem vários serviços de sistema (*daemons*) que, junto com o próprio kernel, gravam regularmente o status do sistema e eventos específicos em arquivos de registro. Dessa maneira, o administrador pode verificar regularmente o status do sistema em um determinado momento, reconhecer erros ou funções defeituosas e solucioná-los com

total precisão. Esses arquivos de registro são normalmente armazenados em /var/log, como especificado pelo FHS, e crescem diariamente. O pacote logrotate ajuda a controlar o crescimento desses arquivos.

Configure o logrotate com o arquivo /etc/logrotate.conf. Em particular, a especificação include configura principalmente os arquivos adicionais a serem lidos. Programas que produzem arquivos de registro instalam arquivos de configuração individuais em /etc/logrotate.d. Por exemplo, esses arquivos vêm com os pacotes apache2 (/etc/logrotate.d/apache2) e syslogd (/etc/logrotate.d/syslog).

***Exemplo 14.3** Exemplo para /etc/logrotate.conf*

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

logrotate é controlado pelo cron e é chamado diariamente por /etc/cron.daily/logrotate.

IMPORTANTE

A opção create lê todas as configurações feitas pelo administrador em /etc/permissions*. Certifique-se de que não haja conflitos devido a modificações pessoais.

14.1.4 O comando locate

locate, um comando para localização rápida de arquivos, não está incluído no escopo padrão do software instalado. Se desejado, instale o pacote findutils-locate. O processo updatedb é iniciado automaticamente a cada noite ou aproximadamente 15 minutos após a inicialização do sistema.

14.1.5 O comando ulimit

Com o comando ulimit (*limites do usuário*), é possível definir limites para o uso dos recursos do sistema e fazer com que sejam exibidos. O ulimit é especialmente útil para limitar a memória disponível para os aplicativos. Com isso, um aplicativo pode ser impedido de absorver recursos em demasia do sistema e deixar o sistema operacional lento ou até travá-lo.

O comando ulimit pode ser usado com várias opções. Para limitar o uso da memória, use as opções listadas na Tabela 14.1, "ulimit: definindo recursos para o usuário" (p 181).

Tabela 14.1 *ulimit: definindo recursos para o usuário*

-m	O tamanho máximo do conjunto residente
-v	A quantidade máxima de memória virtual disponível para o shell
-s	O tamanho máximo da pilha
-c	O tamanho máximo dos arquivos básicos criados
-a	Todos os limites atuais são informados

Entradas globais de sistema podem ser feitas em /etc/profile. Lá, habilite a criação de arquivos básicos (necessários aos programadores para *depuração*). Um usuário normal não pode aumentar os valores especificados em /etc/profile pelo administrador do sistema, mas pode fazer entradas especiais em ~/.bashrc.

***Exemplo 14.4** ulimit: configurações em ~/.bashrc*

```
# Limits maximum resident set size (physical memory):
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

As alocações de memória devem ser especificadas em KB. Para obter informações mais detalhadas, consulte `man bash`.

IMPORTANTE

Nem todos os shells suportam as diretivas `ulimit`. O PAM (por exemplo, `pam_limits`) oferece possibilidades abrangentes de ajustes se você depende de configurações abrangentes para essas restrições.

14.1.6 O comando free

O comando `free` exibe a quantidade total de memória física livre e utilizada e o espaço de troca no sistema, além dos buffers e do cache consumidos pelo kernel. O conceito de *RAM disponível* surgiu antes da época do gerenciamento unificado de memória. O slogan *memória livre é memória ruim* se aplica bem ao Linux. Como resultado, o Linux sempre se esforçou para equilibrar caches externos sem realmente permitir memória livre ou sem uso.

Basicamente, o kernel não tem conhecimento direto de nenhum aplicativo ou dados de usuário. Em vez disso, ele gerencia aplicativos e dados de usuário em um *cache de página*. Se a memória diminuir, partes dele são gravadas na partição de troca ou em arquivos, dos quais podem ser lidas inicialmente com a ajuda do comando `mmap` (consulte `man mmap`).

O kernel também contém outros caches, como o *cache slab*, onde os caches usados para acesso a rede são armazenados. Isso pode explicar as diferenças entre os contadores em `/proc/meminfo`. A maioria deles (mas não todos) pode ser acessada via `/proc/slabinfo`.

No entanto, se o seu objetivo for descobrir quanta RAM está em uso, encontre essa informação em `/proc/meminfo`.

14.1.7 Páginas de manual e de informações

Para alguns aplicativos GNU (como o tar), as páginas de manuais não são mais mantidas. Para esses comandos, use a opção `--help` para obter uma breve visão geral das páginas de informações, que fornecem instruções mais detalhadas. O info é um sistema de hipertexto do GNU. Leia uma introdução sobre esse sistema digitando `infoinfo`. As páginas de informações podem ser exibidas com Emacs digitando `emacs -f info` ou diretamente em um console, com `info`. Também é possível usar tkinfo, xinfo ou o sistema de ajuda do para exibir as páginas de informações.

14.1.8 Selecionando páginas de manual usando o comando man

Para ler a página de manual, digite `man` *`página_de_manual`*. Se existir uma página de manual com o mesmo nome em seções diferentes, elas serão listadas com os números da seção correspondentes. Selecione uma para exibir. Se você não digitar um número de seção em alguns segundos, a primeira página de manual será exibida.

Para mudar desse comportamento para o padrão do sistema, defina `MAN_POSIXLY_CORRECT=1` em um arquivo de inicialização de shell, como `~/.bashrc`.

14.1.9 Configurações para GNU Emacs

O GNU Emacs é um complexo ambiente de trabalho. As seções a seguir descrevem os arquivos de configuração processados quando o GNU Emacs é iniciado. Há mais informações em http://www.gnu.org/software/emacs/.

Na inicialização, o Emacs lê vários arquivos que contêm as configurações do usuário, administrador do sistema e distribuidor para personalização ou pré-configuração. O arquivo de inicialização `~/.emacs` é instalado nos diretórios pessoais dos usuários individuais por meio de `/etc/skel`. O `.emacs`, por sua vez, lê o arquivo `/etc/skel/.gnu-emacs`. Para personalizar o programa, copie o arquivo `.gnu-emacs` para o diretório pessoal (com `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`) e faça as configurações desejadas nesse diretório.

O .gnu-emacs define o arquivo ~/.gnu-emacs-custom como arquivo personalizado. Se os usuários tiverem feito as configurações com as opções personalizar no Emacs, as configurações serão gravadas no arquivo ~/.gnu-emacs-custom.

Com o SUSE Linux Enterprise Desktop, o pacote emacs instala o arquivo site-start.el no diretório /usr/share/emacs/site-lisp. O arquivo site-start.el é carregado antes do arquivo de inicialização ~/.emacs. Entre outras coisas, o arquivo site-start.el assegura que os arquivos de configuração especial distribuídos com os pacotes de expansão do Emacs, como o psgml, sejam carregados automaticamente. Os arquivos de configuração deste tipo também estão localizados em /usr/share/emacs/site-lisp, e sempre começam com o nome suse-start-. O administrador do sistema local pode especificar configurações globais do sistema no arquivo default.el.

Mais informações sobre esses arquivos estão disponíveis no arquivo de informações do Emacs em *Init File*: info:/emacs/InitFile. Informações sobre como desabilitar o carregamento desses arquivos, se necessário, também são fornecidas neste local.

Os componentes do Emacs são divididos em vários pacotes:

- O pacote base emacs.
- emacs-x11 (geralmente instalado): o programa *com* suporte para X11.
- emacs-nox: o programa *sem* suporte para X11.
- emacs-info: documentação online em formato info.
- emacs-el: os arquivos de biblioteca não compilados em Emacs Lisp. Eles não são necessários em tempo de execução.
- Numerosos pacotes complementares podem ser instalados se necessário: emacs-auctex (LaTeX), psgml (SGML e XML), gnuserv (operação cliente e servidor) e outros.

14.2 Consoles virtuais

O Linux é um sistema multiusuário e multitarefa. As vantagens desses recursos podem ser apreciadas mesmo em um sistema de PC independente. No modo de texto, existem seis consoles virtuais disponíveis. Alterne entre eles utilizando a combinação de teclas de Alt + F1 até Alt + F6. O sétimo console é reservado para X e o décimo console mostra as mensagens do kernel. Podem ser atribuídos mais ou menos consoles com a modificação do arquivo `/etc/inittab`.

Para alternar para um console de X sem o fechar, use a combinação de teclas de Ctrl + Alt + F1 até Ctrl + Alt + F6. Para voltar para X, pressione Alt + F7.

14.3 Mapeamento de teclado

Para padronizar o mapeamento de teclado de programas, foram feitas mudanças nos seguintes arquivos:

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.emacs
/etc/skel/.gnu-emacs
/etc/skel/.vimrc
/etc/csh.cshrc
/etc/termcap
/usr/share/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

Essas mudanças afetam apenas os aplicativos que usam as entradas `terminfo` ou que têm arquivos de configuração que são modificados diretamente (`vi`, `emacs`, etc.). Os aplicativos que não acompanham o sistema devem ser adaptados a esses padrões.

Em X, a tecla Compose (multitecla) pode ser habilitada conforme explicado em `/etc/X11/Xmodmap`.

Outras configurações são possíveis utilizando-se a Extensão de Teclado X (XKB). Essa extensão também é usada pelos ambientes de área de trabalho do GNOME (gswitchit) e do KDE (kxkb).

DICA: para obter mais informações

Há informações sobre o XKB disponíveis nos documentos listados em `/usr/share/doc/packages/xkeyboard-config` (parte do pacote `xkeyboard-config`).

14.4 Configurações de idioma e específicas de país

O sistema é, em uma extensão bastante ampla, internacionalizado e pode ser modificado de acordo com as necessidades locais. A internacionalização (*I18N*) permite localizações específicas (*L10N*). As abreviações I18N e L10N são derivadas das primeiras e últimas letras das palavras e, no meio, está o número de letras omitidas.

As configurações são feitas com variáveis `LC_` definidas no arquivo `/etc/sysconfig/language`. Elas referem-se não somente ao *suporte ao idioma nativo*, mas também às categorias *Mensagens* (Idioma), *Conjunto de Caracteres*, *Ordem de Classificação*, *Hora e Data*, *Números* e *Moeda*. Cada uma dessas categorias pode ser definida diretamente com sua própria variável ou indiretamente com uma variável master no arquivo `language` (consulte a página de manual `local`).

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`
: Essas variáveis são passadas para o shell sem o prefixo `RC_` e representam as categorias listadas. Os perfis shell de referência estão listados abaixo. A configuração atual pode ser exibida com o comando `locale`.

`RC_LC_ALL`
: Essa variável, se definida, sobregrava os valores das variáveis já mencionadas.

`RC_LANG`
: Se nenhuma das variáveis anteriores for definida, esse é o fallback. Por padrão, apenas `RC_LANG` está definida. Isso facilita o processo para que os usuários informem seus próprios valores.

ROOT_USES_LANG
: Uma variável yes ou no. Se for definida como no, root sempre funcionará no ambiente POSIX.

As variáveis podem ser definidas com o editor sysconfig do YaST (consulte a Seção 11.3.1, “Mudando a configuração do sistema usando o Editor sysconfig do YaST” (p 140)). O valor dessa variável contém o código do idioma, código do país, codificação e modificador. Os componentes individuais são conectados por caracteres especiais:

```
LANG=<language>[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

14.4.1 Alguns exemplos

Você deve sempre definir os códigos do idioma e do país juntos. As configurações do idioma seguem o padrão ISO 639 disponível em http://www.evertype.com/standards/iso639/iso639-en.html e http://www.loc.gov/standards/iso639-2/. Os códigos de país estão listados em ISO 3166, consulte http://en.wikipedia.org/wiki/ISO_3166.

Só faz sentido definir valores para os quais os arquivos de descrição utilizáveis podem ser encontrados em /usr/lib/locale. Arquivos de descrição adicionais podem ser criados de arquivos em /usr/share/i18n utilizando o comando localedef. Os arquivos de descrição fazem parte do pacote glibc-i18ndata. Um arquivo de descrição para en_US.UTF-8 (para inglês e Estados Unidos) pode ser criado com:

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

LANG=en_US.UTF-8
: Essa é a configuração padrão se Inglês americano for selecionado durante a instalação. Se você tiver selecionado outro idioma, ele será habilitado, mas ainda terá o UTF-8 como codificação de caractere.

LANG=en_US.ISO-8859-1
: Define o idioma como inglês, o país como Estados Unidos e o conjunto de caracteres como ISO-8859-1. Essa definição de caractere não suporta o sinal de Euro, mas às vezes pode ser útil para programas que não foram atualizados para suportar

UTF-8. A string que define o conjunto de caracteres (ISO-8859-1 nesse caso) é então avaliada por programas como o Emacs.

LANG=en_IE@euro
: O exemplo acima inclui explicitamente o sinal de Euro em uma configuração de idioma. Essa configuração está basicamente obsoleta agora, pois o UTF-8 também cobre o símbolo do Euro. Será útil apenas se um aplicativo suportar ISO-8859-15 e não UTF-8.

Nas versões anteriores, era necessário executar SuSEconfig após fazer qualquer mudança em /etc/sysconfig/language. O SuSEconfig então gravava as mudanças em /etc/SuSEconfig/profile e /etc/SuSEconfig/csh.login. No login, esses arquivos eram lidos por /etc/profile (para Bash) ou por /etc/csh.login (para tcsh) .

Nas versões recentes, /etc/SuSEconfig/profile foi substituído por /etc/profile.d/lang.sh, e /etc/SuSEconfig/csh.login por /etc/profile.de/lang.csh. Porém, se eles existirem, ambos arquivos legados ainda serão lidos no login.

A cadeia do processo agora é a seguinte:

- Para Bash: /etc/profile lê /etc/profile.d/lang.sh que, por sua vez, analisa /etc/sysconfig/language.

- Para tcsh: No login, /etc/csh.login lê /etc/profile.d/lang.csh que, por sua vez, analisa /etc/sysconfig/language.

Isso garante que nenhuma mudança em /etc/sysconfig/language fique disponível no próximo login para o respectivo shell, sem precisar executar o SuSEconfig primeiro.

Os usuários anular os padrões do sistema editando o seu ~/.bashrc da maneira adequada. Por exemplo, se você não quiser usar o en_US para mensagens de programa em todo o sistema, inclua LC_MESSAGES=es_ES para que as mensagens sejam exibidas em espanhol.

14.4.2 Configurações locais em ~/.i18n

Se não estiver satisfeito com os padrões do sistema local, mude as configurações em `~/.i18n` de acordo com a sintaxe de script Bash. As entradas em `~/.i18n` substituem os padrões do sistema de `/etc/sysconfig/language`. Use os mesmos nomes de variáveis, mas sem os prefixos de namespace `RC_`. Por exemplo, use `LANG` em vez de `RC_LANG`:

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

14.4.3 Configurações de suporte de idioma

Arquivos na categoria *Mensagens* são, via de regra, armazenados somente no diretório do idioma correspondente (como `en`) para ter um fallback. Se você definir `LANG` para `en_US` e o arquivo de mensagem em `/usr/share/locale/en_US/LC_MESSAGES` não existir, ele voltará para `/usr/share/locale/en/LC_MESSAGES`.

Uma cadeia de fallback também pode ser definida, por exemplo, para bretão para francês ou galego para espanhol para português:

`LANGUAGE="br_FR:fr_FR"`

`LANGUAGE="gl_ES:es_ES:pt_PT"`

Se desejar, use as variantes norueguesas Nynorsk e Bokmål (com fallback adicional para `no`):

`LANG="nn_NO"`

`LANGUAGE="nn_NO:nb_NO:no"`

ou

`LANG="nb_NO"`

`LANGUAGE="nb_NO:nn_NO:no"`

Observe que em norueguês, LC_TIME também é tratado de maneira diferente.

Um problema que pode surgir é um separador usado para delimitar grupos de dígitos não ser reconhecido corretamente. Isso acontece se LANG for definido para um código de idioma com somente duas letras, como de, mas o arquivo de definição que o glibc utiliza estiver localizado em /usr/share/lib/de_DE/LC_NUMERIC. Por isso, LC_NUMERIC deve ser definido como de_DE para tornar a definição de separador visível para o sistema.

14.4.4 Para obter mais informações

- *The GNU C Library Reference Manual*, Capítulo "Locales and Internationalization". Ele está incluído em glibc-info. O pacote está disponível no SUSE Linux Enterprise Software Development Kit (SDK). O SDK é um produto complementar do SUSE Linux Enterprise e está disponível para download pelo site http://download.suse.com/.

- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, atualmente em http://www.cl.cam.ac.uk/~mgk25/unicode.html.

- *Unicode-Howto* por Bruno Haible, disponível em http://tldp.org/HOWTO/Unicode-HOWTO-1.html.

15 Operação da impressora

O SUSE® Linux Enterprise Desktop suporta a impressão com muitos tipos de impressoras, incluindo impressoras de rede remotas. É possível configurar as impressoras manualmente ou com o YaST. Para obter instruções de configuração, consulte a Section “Setting Up a Printer” (Chapter 5, *Setting Up Hardware Components with YaST*, ↑*Deployment Guide*). Os utilitários gráficos e de linha de comando estão disponíveis para iniciar e gerenciar serviços de impressão. Se a sua impressora não funcionar como se esperava, consulte a Seção 15.7, “Solução de problemas” (p 201).

CUPS (Common Unix Printing System) é o sistema de impressão padrão no SUSE Linux Enterprise Desktop.

As impressoras podem ser distinguidas pela interface, como USB ou rede, e pela linguagem de impressão. Ao comprar uma impressora, verifique se há no seu hardware uma interface (como porta USB ou paralela) disponível para ela e uma linguagem de impressora adequada. As impressoras podem ser categorizadas com base em três classes de linguagem:

Impressoras PostScript
: PostScript é a linguagem de impressora na qual a maior parte dos serviços de impressão em Linux e Unix são gerados e processados pelo sistema de impressão interno. Se documentos PostScript puderem ser diretamente processados pela impressora e não precisarem ser convertidos em estágios adicionais do sistema de impressão, o número de origens de erro potenciais será reduzido.

Impressora padrão (linguagens como PCL e ESC/P)
: Embora essas linguagens de impressora tenham surgido há bastante tempo, ainda são usadas e sofrem constantes desenvolvimentos para se adaptarem aos novos

recursos de impressoras. No caso de linguagens conhecidas, o sistema pode converter tarefas de impressão PostScript na respectiva linguagem de impressão com a ajuda do Ghostscript. Esse estágio de processamento é chamado de interpretação. As linguagens mais conhecidas são PCL (mais usada pelas impressoras HP e seus clones) e ESC/P (utilizada nas impressoras Epson). Geralmente, essas linguagens são suportadas no Linux e produzem um resultado de impressão adequado. O Linux pode não conseguir realizar algumas funções especiais da impressora. A não ser pelo projeto HP developing HPLIP (HP Linux Imaging and Printing), não há fabricantes de impressora que desenvolvem e disponibilizam drivers de Linux aos distribuidores Linux sob uma licença de código-fonte aberto.

Impressoras proprietárias (também denominadas impressoras GDI)
: Essas impressoras não suportam nenhuma das linguagens de impressora comuns. Elas usam suas próprias linguagens de impressora não documentadas, que ficam sujeitas a mudanças quando é lançada uma edição nova de um modelo. Geralmente, apenas os drivers do Windows estão disponíveis para essas impressoras. Consulte a Seção 15.7.1, "Impressoras sem suporte de linguagem de impressora padrão" (p 201) para obter mais informações.

Antes de comprar uma nova impressora, consulte as seguintes fontes para verificar a abrangência do suporte ao equipamento pretendido:

`http://www.linuxfoundation.org/OpenPrinting/`
: A home page OpenPrinting com o banco de dados de impressão. O banco de dados mostra o status mais recente de suporte do Linux. No entanto, a distribuição do Linux só pode integrar os drivers disponíveis no momento da produção. Da mesma forma, uma impressora atualmente classificada como "perfeitamente suportada" talvez não apresentasse esse status quando a versão mais recente do SUSE Linux Enterprise Desktop foi lançada. Assim, os bancos de dados não indicarão necessariamente o status correto, mas apenas uma informação aproximada.

`http://pages.cs.wisc.edu/~ghost/`
: Página do Ghostscript na Web.

`/usr/share/doc/packages/ghostscript-library/catalog.devices`
: Listas de drivers incluídos.

15.1 Fluxo de trabalho do sistema de impressão

O usuário cria um serviço de impressão. O serviço de impressão consiste nos dados a serem impressos e nas informações para o spooler, como nome da impressora ou nome da fila de impressão e, opcionalmente, nas informações para o filtro, como opções específicas da impressora.

Existe pelo menos uma fila de impressão dedicada para cada impressora. O spooler mantém o serviço de impressão em fila até que a impressora desejada esteja pronta para receber dados. Uma vez pronta, o spooler envia os dados pelo filtro, tendo a impressora como back end.

O filtro converte os dados gerados pelo aplicativo que está imprimindo (geralmente PostScript ou PDF, mas também ASCII, JPEG e outros) em dados específicos da impressora (PostScript, PCL, ESC/P etc.). Os recursos da impressora são descritos nos arquivos PPD. O arquivo PPD contém opções da impressora com os parâmetros necessários para habilitá-los. O sistema de filtros verifica se as opções selecionadas pelo usuário foram habilitadas.

Se você usa uma impressora PostScript, o sistema de filtros converte os dados em PostScript específico da impressora. Isso não exige um driver de impressora. Se você usa uma impressora não PostScript, o sistema de filtros converte os dados em dados específicos da impressora. Isso exige um driver adequado à sua impressora. O back end recebe do filtro os dados específicos da impressora e os repassa a ela.

15.2 Métodos e protocolos de conexão de impressoras

Existem várias possibilidades para conectar uma impressora ao sistema. A configuração do sistema de impressão CUPS não faz distinção entre uma impressora local e uma impressora conectada ao sistema pela rede.

ATENÇÃO: mudando as conexões de cabo em um sistema em execução

Ao conectar a impressora à máquina, não esqueça de que apenas dispositivos USB podem ser conectados ou desconectados durante a operação. Para evitar danos ao sistema ou à impressora, encerre o sistema antes de mudar qualquer conexão que não seja USB.

15.3 Instalando o software

PPD (descrição de impressora PostScript) é a linguagem de computador que descreve as propriedades, como resolução, e as opções, como disponibilidade de uma unidade duplex. Essas descrições são necessárias para o uso de várias opções de impressora no CUPS. Sem um arquivo PPD, os dados de impressão seriam encaminhados à impressora em estado “bruto”, o que normalmente não é desejado. Durante a instalação do SUSE Linux Enterprise Desktop, muitos arquivos PPD são pré-instalados.

Para configurar uma impressora PostScript, a melhor opção é obter um arquivo PPD adequado. Há vários arquivos PPD disponíveis no pacote de `PPDs do fabricante`, que são automaticamente instalados no escopo da instalação padrão. Consulte a Seção 15.6.2, “Arquivos PPD em pacotes diferentes” (p 199) e a Seção 15.7.2, “Nenhum arquivo PPD adequado disponível para impressora PostScript” (p 202).

É possível armazenar novos arquivos PPD no diretório `/usr/share/cups/model/` ou adicioná-los ao sistema de impressão com o YaST, conforme descrito na Section “Adding Drivers with YaST” (Chapter 5, *Setting Up Hardware Components with YaST*, ↑*Deployment Guide*). Na sequência, é possível selecionar o arquivo PPD durante a configuração da impressora.

Observe se o fabricante da impressora requer que você instale pacotes inteiros de software. Primeiro, esse tipo de instalação pode resultar na perda do suporte oferecido pelo SUSE Linux Enterprise Desktop e, segundo, os comandos de impressão podem funcionar de forma diferente e o sistema pode não conseguir mais trabalhar com dispositivos de outros fabricantes. Por isso, não recomendamos instalar o software do fabricante.

15.4 Impressoras de rede

Uma impressora de rede pode suportar vários protocolos, alguns deles simultaneamente. Embora a maioria dos protocolos suportados seja padronizada, alguns fabricantes modificam o padrão. Os fabricantes então fornecem drivers apenas para alguns sistemas operacionais. Infelizmente, raros são os drivers para Linux. Na situação atual, não é possível agir como se todos os protocolos funcionassem perfeitamente no Linux. Portanto, talvez seja necessário testar várias opções para obter uma configuração funcional.

O CUPS suporta os protocolos `socket`, `LPD`, `IPP` e `smb`.

socket
: *Socket* refere-se a uma conexão em que os dados de impressão simples são enviados diretamente a um soquete TCP. Alguns dos números de portas de soquete normalmente usados são `9100` ou `35`. A sintaxe do URI (uniform resource identifier) do dispositivo é: socket://*`IP.da.impressora`*:*`porta`*, por exemplo: `socket://192.168.2.202:9100/`.

LPD (Line Printer Daemon)
: O protocolo LPD está descrito no RFC 1179. Nesse protocolo, alguns dados relacionados ao serviço, como o ID da fila de impressão, são enviados antes dos dados da impressão propriamente ditos. Portanto, a fila de impressão deve ser especificada no momento da configuração do protocolo LPD. As implementações de fabricantes de impressoras diferentes são flexíveis o suficiente para aceitar qualquer nome como a fila de impressão. Se necessário, o manual da impressora indicará o nome a ser usado. Geralmente se usa LPT, LPT1, LP1 ou nomes semelhantes. O número de porta para o serviço LPD é `515`. Um exemplo de URI de dispositivo é `lpd://192.168.2.202/LPT1`.

IPP (Internet Printing Protocol)
: IPP é um protocolo relativamente novo (1999) baseado no protocolo HTTP. Com o IPP, mais dados referentes à tarefa são transmitidos. O CUPS usa o IPP em transmissões internas de dados. É necessário indicar o nome da fila de impressão para que o IPP seja configurado corretamente. A porta padrão do IPP é `631`. Exemplos de URIs de dispositivo: `ipp://192.168.2.202/ps` e `ipp://192.168.2.202/impressoras/ps`.

SMB (compartilhamento Windows)
: O CUPS também suporta a impressão em impressoras conectadas a compartilhamentos Windows. O protocolo usado para essa finalidade é o SMB. O SMB usa os números de porta `137`, `138` e `139`. Exemplos de URIs de dispositivo: `smb://usuário:senha@grupo_de_trabalho/smb.exemplo.com/printer`, `smb://usuário:senha@smb.exemplo.com/impressora` e `smb://smb.exemplo.com/impressora`.

O protocolo suportado pela impressora deve ser determinado antes da configuração. Se o fabricante não fornecer as informações necessárias, o comando `nmap` (que vem com o pacote `nmap`) pode ser usado para verificar o protocolo. O `nmap` verifica se há portas abertas em um host. Por exemplo:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

15.4.1 Configurando o CUPS com ferramentas da linha de comando

É possível configurar o CUPS com ferramentas de linha de comando, como `lpinfo`, `lpadmin` e `lpoptions`. Você precisa de um URI de dispositivo composto por um back end, como uma porta paralela, e parâmetros. Para determinar os URIs de dispositivo válidos no sistema, use o comando `lpinfo -v | grep ":/"`:

```
# lpinfo -v | grep ":/"
direct usb://ACME/FunPrinter%20XL
direct parallel:/dev/lp0
```

Com o `lpadmin`, o administrador do servidor CUPS pode adicionar, remover ou gerenciar filas de impressão. Para adicionar uma fila de impressão, use a seguinte sintaxe:

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

Em seguida, o dispositivo (`-v`) fica disponível como *`fila`* (`-p`), usando o arquivo PPD especificado (`-P`). Isso significa que você precisa saber qual é o arquivo PPD e o URI de dispositivo para configurar a impressora manualmente.

Não use `-E` como primeira opção. Em todos os comandos CUPS, `-E` como primeiro argumento define o uso de uma conexão criptografada. Para habilitar a impressora, `-E` deve ser usado como mostrado no seguinte exemplo:

```
lpadmin -p ps -v parallel:/dev/lp0 -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

O seguinte exemplo configura uma impressora de rede:

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Para conhecer mais opções de `lpadmin`, consulte a página de manual de `lpadmin(8)`.

Durante a configuração da impressora, algumas opções são definidas como padrão. Essas opções podem ser modificadas para cada serviço de impressão (dependendo da ferramenta de impressão utilizada). Também é possível modificar essas opções padrão com o YaST. Usando ferramentas de linha de comando, defina opções padrão da seguinte forma:

1 Primeiro, liste todas as opções:

```
lpoptions -p queue -l
```

Exemplo:

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

A opção padrão ativada é identificada por um asterisco na frente (`*`).

2 Mude a opção com `lpadmin`:

```
lpadmin -p queue -o Resolution=600dpi
```

3 Verifique a nova configuração:

```
lpoptions -p queue -l
```

```
Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

Quando um usuário comum executa `lpoptions`, as configurações são gravadas em `~/.cups/lpoptions`. Porém, as configurações de `root` são gravadas em `/etc/cups/lpoptions`.

15.5 Imprimindo pela linha de comando

Para imprimir pela linha de comando, digite `lp-d` *`nome da fila nome do arquivo`*, substituindo *`nome da fila`* e *`nome do arquivo`* pelos nomes correspondentes.

Alguns aplicativos dependem do comando `lp` para imprimir. Nesse caso, digite o comando correto na caixa de diálogo do aplicativo, geralmente sem especificar *`nome do arquivo`*, por exemplo `lp -d`*`nome da fila`*.

15.6 Recursos especiais no SUSE Linux Enterprise Desktop

Vários recursos do CUPS foram adaptados para o SUSE Linux Enterprise Desktop. Algumas das mudanças mais importantes são abordadas aqui.

15.6.1 CUPS e firewall

Após realizar a instalação padrão do SUSE Linux Enterprise Desktop, o SuSEFirewall2 será ativado e as interfaces de rede serão configuradas para ficarem na `Zona Externa`, que bloqueia o tráfego de entrada. Há mais informações sobre a configuração do SuSEFirewall2 disponíveis na Section “SuSEfirewall2” (Chapter 15, *Masquerading and Firewalls*, ↑*Security Guide*) e em `http://en.opensuse.org/SDB:CUPS_and_SANE_Firewall_settings`.

15.6.1.1 Cliente CUPS

Normalmente, um cliente CUPS é executado em uma estação de trabalho comum, localizada em um ambiente de rede confiável protegido por firewall. Neste caso, é recomendável configurar a interface de rede para ficar na `Zona Interna`, de modo que a estação de trabalho possa ser alcançada de dentro da rede.

15.6.1.2 Servidor CUPS

Se o servidor CUPS fizer parte de um ambiente de rede confiável, protegido por um firewall, a interface de rede deverá ser configurada para ficar na `Zona Interna` do firewall. Não é recomendado configurar um servidor CUPS em um ambiente de rede não confiável, a menos que você tenha o cuidado de mantê-lo protegido por regras especiais de firewall e opções seguras na configuração do CUPS.

15.6.2 Arquivos PPD em pacotes diferentes

A configuração de impressora do YaST define as filas do CUPS usando os arquivos PPD instalados em `/usr/share/cups/model`. Para localizar os arquivos PPD adequados ao modelo da impressora, o YaST compara o fornecedor e o modelo determinados durante a detecção de hardware com os fornecedores e modelos em todos os arquivos PPD. Para isso, a configuração de impressora do YaST gera um banco de dados com as informações de fabricante e modelo extraídas dos arquivos PPD.

A configuração com apenas arquivos PPD e nenhuma outra fonte de informação tem a vantagem de permitir a livre modificação de arquivos PPD em `/usr/share/cups/model/`. Por exemplo, se você tem apenas impressoras PostScript, normalmente não precisa dos arquivos PPD Foomatic do pacote `cups-drivers` ou os arquivos PPD Gutenprint do pacote `gutenprint`. Em vez disso, os arquivos PPD das suas impressoras PostScript podem ser copiados diretamente para `/usr/share/cups/model` (se já não existirem no pacote `manufacturer-PPDs`) para proporcionarem uma configuração ideal às impressoras.

15.6.2.1 Arquivos PPD do CUPS do pacote `cups`

Os arquivos PPD genéricos do pacote `cups` foram complementados com arquivos PPD Foomatic adaptados para impressoras PostScript nível 1 e 2:

- `/usr/share/cups/model/Postscript-level1.ppd.gz`
- `/usr/share/cups/model/Postscript-level2.ppd.gz`

15.6.2.2 Arquivos PPD do pacote cups-drivers

Normalmente, o filtro de impressora Foomatic foomatic-rip é usado junto com Ghostscript para impressoras não PostScript. Os arquivos PPD Foomatic adequados possuem as entradas *NickName: ... Foomatic/Ghostscript driver e *cupsFilter: ... foomatic-rip. Esses arquivos PPD estão localizados no pacote cups-drivers.

O YaST geralmente prefere um arquivo manufacturer-PPD. Entretanto, quando não existe nenhum arquivo manufacturer-PPD adequado, um arquivo PPD Foomatic com entrada *NickName: ... Foomatic ... (recommended) é selecionado.

15.6.2.3 Arquivos PPD Gutenprint do pacote gutenprint

Em vez de foomatic-rip, o filtro CUPS rastertogutenprint do Gutenprint (antes conhecido como GIMP-Print) pode ser usado em várias impressoras não PostScript. Esse filtro e os arquivos PPD Gutenprint adequados estão disponíveis no pacote gutenprint. Os arquivos PPD Gutenprint estão localizados em /usr/share/cups/model/gutenprint/ e possuem as entradas *NickName: ... CUPS+Gutenprint e *cupsFilter: ... rastertogutenprint.

15.6.2.4 Arquivos PPD de fabricantes de impressoras no pacote manufacturer-PPDs

O pacote manufacturer-PPDs contém arquivos PPD de fabricantes de impressoras que são liberados mediante uma licença suficientemente permissiva. Impressoras PostScript devem ser configuradas com o arquivo PPD adequado do fabricante da impressora, já que esse arquivo permite o uso de todas as funções da impressora PostScript. O YaST prefere um arquivo PPD dos manufacturer-PPDs. O YaST não poderá usar um arquivo PPD do pacote manufacturer-PPDs se o nome do modelo não for correspondente. Isso poderá ocorrer se o pacote manufacturer-PPDs contiver apenas um arquivo PPD para modelos semelhantes, como a série Funprinter 12xx. Nesse caso, selecione manualmente o arquivo PPD correspondente no YaST.

15.7 Solução de problemas

As seções a seguir abordam alguns dos problemas mais encontrados em relação a hardware e software de impressora, bem como formas de solucionar ou superar esses problemas. Os tópicos abordados incluem impressoras GDI, arquivos PPD e configuração de porta. Problemas comuns de impressoras de rede, impressões com defeito e gerenciamento de filas também são tratados.

15.7.1 Impressoras sem suporte de linguagem de impressora padrão

Essas impressoras não suportam nenhuma linguagem de impressora comum, podendo apenas ser tratadas com sequências especiais de controle proprietário. Portanto, elas só funcionam com as versões de sistema operacional para as quais o fabricante fornece driver. GDI é uma interface de programação desenvolvida pela Microsoft* para dispositivos gráficos. Geralmente o fabricante fornece drivers apenas para Windows e, com o driver do Windows usa a interface GDI, essas impressoras também são chamadas de *impressoras GDI*. O verdadeiro problema não é a interface de programação, mas o fato de que tais impressoras só podem ser tratadas com a linguagem de impressora proprietária do respectivo modelo de impressora.

Algumas impressoras GDI podem ser ajustadas para funcionar no modo GDI ou em uma das linguagens de impressora padrão. Consulte o manual da impressora para saber se isso é possível. Alguns modelos exigem software especial do Windows para fazer o ajuste (observe que o driver de impressora do Windows pode sempre retornar a impressora para o modo GDI quando se imprime do Windows). Para outras impressoras GDI, existem módulos de extensão disponíveis para uma linguagem de impressora padrão.

Alguns fabricantes oferecem drivers proprietários para suas impressoras A desvantagem dos drivers de impressora proprietários é que não há garantia de que vão funcionar com o sistema de impressão instalado ou de que sejam adequados para as diferentes plataformas de hardware. Em contraste, impressoras que suportam uma linguagem de impressora padrão não dependem de uma versão do sistema de impressão especial ou de plataforma de hardware especial.

Em vez de perder tempo tentando fazer funcionar um driver de Linux proprietário, a compra de uma impressora que suporte a linguagem padrão de impressora (preferencialmente PostScript) pode ter melhor custo-benefício. Isso solucionaria o problema do driver de uma vez por todas, eliminando a necessidade de instalar e configurar software de driver especial e obter atualizações do driver eventualmente necessárias devido a novos avanços no sistema de impressão.

15.7.2 Nenhum arquivo PPD adequado disponível para impressora PostScript

Se o pacote `manufacturer-PPDs` não incluir o arquivo PPD adequado para uma impressora PostScript, será possível utilizar o arquivo PPD do CD do driver do fabricante da impressora ou fazer download de um arquivo PPD adequado da página do fabricante da impressora na Web.

Se o arquivo PPD for fornecido como arquivo compactado (.zip) ou arquivo compactado de autoextração (`.exe`), faça a descompactação com `unzip`. Primeiro, reveja os termos de licença do arquivo PPD. Em seguida, use o utilitário `cupstestppd` para verificar se o arquivo PPD atende à “Especificação de Formato de Arquivo PPD (PostScript Printer Description — Descrição de Impressora PostScript) da Adobe, versão 4.3”. Se o utilitário retornar “FAIL”, significa que os erros nos arquivos PPD são graves e provavelmente causam os principais problemas. Os problemas reportados pelo `cupstestppd` devem ser eliminados. Se necessário, peça o arquivo PPD adequado ao fabricante da impressora.

15.7.3 Portas paralelas

A abordagem mais segura é conectar a impressora diretamente à primeira porta paralela e selecionar as configurações de porta paralela no BIOS:

- Endereço de E/S: `378` (hexadecimal)
- Interrupção: irrelevante
- Modo: `Normal`, `SPP` ou `Output Only`
- DMA: desabilitado

Se a impressora não puder ser endereçada na porta paralela apesar dessas configurações, digite o endereço de E/S explicitamente de acordo com a configuração no BIOS no formato `0x378` em `/etc/modprobe.conf`. Se houver duas portas paralelas definidas para os endereços de E/S `378` e `278` (hexadecimal), digite-os no formato `0x378,0x278`.

Se a interrupção `7` estiver livre, poderá ser ativada com a entrada mostrada no Exemplo 15.1, “`/etc/modprobe.conf`: Modo de interrupção para a primeira porta paralela” (p 203). Antes de ativar o modo de interrupção, verifique o arquivo `/proc/interrupts` para ver quais interrupções já estão sendo usadas. Somente as interrupções usadas atualmente são exibidas. Isso pode mudar dependendo dos componentes de hardware ativos. A interrupção da porta paralela não deve ser usada por outro dispositivo. Se não tiver certeza, use o modo de polling com `irq=none`.

Exemplo 15.1 *`/etc/modprobe.conf`: Modo de interrupção para a primeira porta paralela*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

15.7.4 Conexões da impressora de rede

Identificação de problemas de rede
: Conecte a impressora diretamente ao computador. Para fins de teste, configure-a como impressora local. Se isso funcionar, o problema está na rede.

Verificando a rede TCP/IP
: A rede TCP/IP e a resolução de nomes devem ser funcionais.

Verificando um `lpd` remoto
: Use o comando a seguir para testar o estabelecimento de uma conexão TCP com `lpd` (porta `515`) no *`host`*.

```
netcat -z host 515 && echo ok || echo failed
```

Se a conexão com `lpd` não for estabelecida, o `lpd` pode não estar ativo ou pode haver problemas básicos de rede.

Como usuário root, use o seguinte comando para consultar um relatório de status (possivelmente muito longo) sobre a *fila* no *host* remoto, considerando que o respectivo lpd esteja ativo e o host aceite consultas:

```
echo -e "\004queue" \
| netcat -w 2 -p 722 host 515
```

Se o lpd não responder, ele pode não estar ativo ou pode haver problemas básicos de rede. Se o lpd responder, a resposta deverá mostrar por que não é possível imprimir na fila do host. Se você receber uma resposta como esta, mostrada no Exemplo 15.2, "Mensagem de erro do lpd" (p 204), significa que o problema está sendo causado pelo lpd remoto.

***Exemplo 15.2** Mensagem de erro do lpd*

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

Verificando um cupsd remoto

Um servidor de rede CUPS pode transmitir suas filas por padrão a cada 30 segundos na porta UDP 631. Conforme apresentado, os seguintes comandos podem ser usados para testar se existe um servidor de rede CUPS de broadcasting na rede. Não deixe de parar seu daemon CUPS local antes de executar o comando.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Se existir um servidor de rede CUPS de transmissão, a saída aparecerá conforme mostrado no Exemplo 15.3, "Transmissão do servidor de rede CUPS" (p 204).

***Exemplo 15.3** Transmissão do servidor de rede CUPS*

```
ipp://192.168.2.202:631/printers/queue
```

Use o comando a seguir para testar o estabelecimento de uma conexão TCP com cupsd (porta 631) no *host*.

```
netcat -z host 631 && echo ok || echo failed
```

Se não for possível estabelecer a conexão com cupsd, pode ser que o cupsd não esteja ativo ou existam problemas básicos de rede. lpstat -h *host* -l -t retorna um relatório de status (possivelmente muito longo) de todas as filas do *host*, contanto que o respectivo cupsd esteja ativo e o host aceite consultas.

O próximo comando pode ser usado para testar se a *fila* do *host* aceita um serviço de impressão que consiste em um único caractere de retorno de carro. Nada será impresso. Possivelmente, será ejetada uma página em branco.

```
echo -en "\r" \
| lp -d queue -h host
```

Solução de problemas da impressora de rede ou da caixa do servidor de impressão

Algumas vezes, spoolers executados na caixa do servidor de impressão causam problemas quando precisam lidar com vários serviços de impressão. Como isso é causado pelo spooler na caixa do servidor de impressão, não há como resolver essa questão. Como solução alternativa, desvie o spooler na caixa do servidor de impressão endereçando a impressora conectada à caixa diretamente com o soquete TCP. Consulte a Seção 15.4, “Impressoras de rede” (p 195).

Dessa forma, a caixa do servidor de impressão é reduzida a um conversor entre as várias formas de transferência de dados (conexão de rede TCP/IP e impressora local). Para usar esse método, você precisa conhecer a porta TCP da caixa do servidor de impressão. Se a impressora estiver conectada à caixa do servidor de impressão e ligada, a porta TCP poderá ser determinada normalmente com o utilitário `nmap` do pacote `nmap`, algum tempo depois que a caixa for ativada. Por exemplo, `nmap`*`endereço_IP`* `pode resultar na seguinte saída para uma caixa do servidor de impressão:`

```
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
515/tcp    open        printer
631/tcp    open        cups
9100/tcp   open        jetdirect
```

Essa saída indica que a impressora conectada à caixa do servidor de impressão pode ser endereçada via soquete TCP na porta `9100`. Por padrão, `nmap` verifica somente algumas portas mais conhecidas listadas em `/usr/share/nmap/nmap-services`. Para verificar todas as portas possíveis, use o comando `nmap-p` *`porta_de_origem-porta_de_destino endereço_IP`*. O processo pode levar algum tempo. Para obter mais informações, consulte a página de manual de `nmap`.

Digite um comando como

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

para enviar strings de caracteres ou arquivos diretamente à respectiva porta para testar se a impressora pode ser endereçada dessa porta.

15.7.5 Defeitos na impressão sem mensagem de erro

Para o sistema de impressão, o serviço de impressão é concluído quando o back end do CUPS conclui a transferência de dados ao destinatário (impressora). Se houver falha no processamento posterior no destinatário (por exemplo, se a impressora não imprimir seus próprios dados específicos), o sistema de impressão não notará. Se a impressora não imprimir seus próprios dados específicos, selecione um arquivo PPD mais adequado à impressora.

15.7.6 Filas desabilitadas

Se a transferência de dados para o destinatário falhar completamente após várias tentativas, o back end do CUPS, como `USB` ou `socket`, reportará um erro ao sistema de impressão (ao `cupsd`). O back end determina quantas tentativas malsucedidas são necessárias para que a transferência de dados seja considerada impossível. Visto que as tentativas posteriores serão inúteis, o `cupsd` desabilita a impressão da fila correspondente. Após resolver a causa do problema, o administrador do sistema deve reabilitar a impressão com o comando `cupsenable`.

15.7.7 Navegação do CUPS: apagando serviços de impressão

Se um servidor de rede CUPS transmitir suas filas aos hosts de clientes via navegação e um `cupsd` local adequado estiver ativo nos hosts de clientes, o `cupsd` de cliente aceitará serviços de impressão de aplicativos e os encaminhará ao `cupsd` no servidor. Quando `cupsd` no servidor aceitar um serviço de impressão, ele receberá um novo número de serviço. Portanto, o número da tarefa no host cliente é diferente do número da tarefa no servidor. Como geralmente um serviço de impressão é encaminhado de imediato, não é possível apagá-lo com o número de serviço do host cliente, porque o

cupsd do cliente considera o serviço como concluído assim que ele é encaminhado ao cupsd do servidor.

Para apagar o serviço de impressão do servidor, use um comando como lpstat -h cups.example.com -o para determinar o número do serviço no servidor, contanto que o servidor ainda não tenha concluído o serviço de impressão (isto é, não o tenha enviado inteiramente para a impressora). Com esse número, o serviço de impressão pode ser apagado no servidor:

```
cancel -h cups.example.com queue-jobnumber
```

15.7.8 Serviços de impressão com defeito e erros de transferência de dados

Se você desligar a impressora ou encerrar o computador durante o processo de impressão, o serviço de impressão permanecerá na fila. A impressão continua quando o computador (ou a impressora) é ligado novamente. Os serviços de impressão com defeito devem ser removidos da fila com cancel.

Se o serviço de impressão apresentar defeito ou se ocorrer um erro na comunicação entre o host e a impressora, a impressora imprimirá várias folhas de papel com caracteres ininteligíveis, pois não consegue processar os dados corretamente. Para corrigir essa situação, siga as etapas a seguir:

1 Para interromper a impressão, remova todo o papel das bandejas da impressora jato de tinta ou laser. Impressoras de alta qualidade têm um botão de cancelamento da impressão.

2 O serviço de impressão pode ainda estar na fila, já que os serviços apenas são removidos depois de inteiramente enviados à impressora. Use lpstat -o ou lpstat -h cups.example.com -o para verificar a fila que está sendo impressa. Apague o serviço de impressão com cancel *fila-númerodoserviço* ou cancel -h cups.exemplo.com *fila-númerodoserviço*.

3 Alguns dados podem ainda ser transferidos à impressora mesmo que o serviço tenha sido apagado da fila. Verifique se há um processo back end do CUPS em execução para a fila respectiva e termine-o. Por exemplo, para uma impressora conectada à

porta paralela, o comando `fuser -k /dev/lp0` pode ser usado para terminar todos os processos que ainda estão acessando a impressora (mais precisamente, a porta paralela).

4 Reinicialize a impressora completamente deixando-a desligada por um tempo. Em seguida, insira o papel e ligue a impressora.

15.7.9 Depuração do sistema de impressão do CUPS

Use o seguinte procedimento genérico para localizar problemas no sistema de impressão do CUPS:

1 Defina `LogLevel debug` em `/etc/cups/cupsd.conf`.

2 Pare o `cupsd`.

3 Remova `/var/log/cups/error_log*` para não precisar procurar em arquivos de registro muito grandes.

4 Inicie o `cupsd`.

5 Repita a ação que causou o problema.

6 Verifique as mensagens em `/var/log/cups/error_log*` para identificar a causa do problema.

15.7.10 Para obter mais informações

Há soluções para vários problemas específicos no SUSE Knowledgebase (http://www.suse.com/support/). Localize os artigos relevantes com uma pesquisa pelo texto `CUPS`.

Gerenciamento dinâmico de dispositivos do Kernel com `udev`

16

O kernel pode adicionar ou remover praticamente qualquer dispositivo em um sistema em execução. Mudanças no estado do dispositivo (se um dispositivo foi conectado ou removido) precisam ser estendidas ao espaço do usuário. Os dispositivos deverão ser configurados assim que forem conectados e reconhecidos. Os usuários de um determinado dispositivo precisam ser informados sobre qualquer mudança no estado reconhecido desse dispositivo. O udev fornece a infraestrutura necessária para manter dinamicamente os arquivos dos nós de dispositivo e os links simbólicos no diretório `/dev`. As regras do `udev` fornecem uma maneira de conectar ferramentas externas ao processamento de evento do dispositivo de kernel. Permite personalizar o gerenciamento de dispositivos do `udev`; por exemplo, adicionando determinados scripts para execução como parte do gerenciamento de dispositivos do kernel ou para solicitação e importação de dados adicionais para avaliar durante o gerenciamento de dispositivos.

16.1 O diretório /dev

Os nós de dispositivo no diretório `/dev` fornecem acesso aos dispositivos de kernel correspondentes. Com `udev`, o diretório `/dev` reflete o estado atual do kernel. Cada dispositivo de kernel tem um arquivo de dispositivo correspondente. Se um dispositivo for desconectado do sistema, o nó de dispositivo será removido.

O conteúdo do diretório `/dev` será mantido em um sistema de arquivos temporário, e todos os arquivos serão renderizados a cada inicialização do sistema. Arquivos criados ou modificados manualmente por definição não resistem a uma reinicialização. Diretórios

e arquivos estáticos que sempre devem estar presentes no diretório /dev, independentemente do estado do dispositivo de kernel correspondente, podem ser colocados no diretório /lib/udev/devices. Na inicialização do sistema, o conteúdo do diretório é copiado para o diretório /dev com propriedade e permissões iguais às dos arquivos em /lib/udev/devices.

16.2 uevents e udev do Kernel

As informações de dispositivo necessárias são exportadas pelo sistema de arquivos sysfs. Para cada dispositivo detectado e inicializado pelo kernel, um diretório com o nome do dispositivo é criado. Ele contém arquivos de atributos com propriedades específicas do dispositivo.

Sempre que um dispositivo é adicionado ou removido, o kernel envia um uevent para notificar o udev sobre a mudança. O daemon udev lê e analisa todas as regras especificadas nos arquivos /etc/udev/rules.d/*.rules uma vez na inicialização e as mantém na memória. Se os arquivos de regras são mudados, adicionados ou removidos, o daemon pode recarregar a representação na memória de todas as regras com o comando udevadm control reload_rules. Isso também é feito ao executar /etc/init.d/boot.udev reload. Para obter mais detalhes sobre as regras do udev e sua sintaxe, consulte a Seção 16.6, “Influenciando o gerenciamento de eventos de dispositivo do Kernel com as regras do udev” (p 213).

Cada evento recebido é comparado com o conjunto de regras fornecido. As regras podem adicionar ou modificar chaves de ambiente de eventos, solicitar um nome específico a ser criado pelo nó de dispositivo, adicionar symlinks apontando para o nó ou adicionar programas a serem executados após a criação do nó do dispositivo. Os uevents de núcleo do driver são recebidos de um soquete netlink do kernel.

16.3 Drivers, módulos de kernel e dispositivos

Os drivers de barramento de kernel pesquisam dispositivos. Para cada dispositivo detectado, o kernel cria uma estrutura de dispositivo interna enquanto o núcleo do driver envia um uevent ao daemon udev. Dispositivos de barramento se identificam através

de um ID formatado especialmente, que informa o tipo de dispositivo. Geralmente esses IDs consistem em IDs de produto e fornecedor, além de outros valores específicos do subsistema. Cada barramento tem seu próprio esquema para esses IDs, chamados MODALIAS. O kernel toma as informações do dispositivo, compõe uma string de ID MODALIAS a partir dele e envia essa string junto com o evento. Para um mouse USB, a string tem a seguinte aparência:

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

Cada driver de dispositivo carrega uma lista de álias conhecidos para os dispositivos que pode tratar. A lista está contida no próprio arquivo de módulo de kernel. O programa depmod lê as listas de ID e cria o arquivo modules.alias no diretório /lib/modules do kernel para todos os módulos disponíveis atualmente. Com essa infraestrutura, carregar o módulo é fácil como chamar modprobe para cada evento com uma chave MODALIAS. Se modprobe $MODALIAS for chamado, ele corresponderá o álias do dispositivo composto para o dispositivo com os álias fornecidos pelos módulos. Se uma entrada correspondente for encontrada, o módulo será carregado. Tudo isso é acionado automaticamente pelo udev.

16.4 Inicialização e configuração do dispositivo inicial

Todos os eventos de dispositivo que ocorrem durante o processo de boot antes da execução do daemon udev são perdidos, pois a infraestrutura para gerenciar esses eventos reside no sistema de arquivos raiz e não está disponível naquele momento. Para cobrir essa perda, o kernel fornece um arquivo uevent localizado no diretório de dispositivo de cada dispositivo no sistema de arquivos sysfs. Ao gravar add para esse arquivo, o kernel envia novamente o mesmo evento como o evento perdido durante a inicialização. Um loop simples em todos os arquivos uevent em /sys aciona todos os eventos novamente para criar os nós de dispositivo e executar a configuração do dispositivo.

Por exemplo, durante o boot, um mouse USB talvez não seja inicializado pela lógica de boot anterior, pois o driver não está disponível nesse momento. O evento para a descoberta do dispositivo foi perdido e não encontrou um módulo de kernel para o dispositivo. Em vez de pesquisar manualmente pelos dispositivos possivelmente conectados, o udev apenas solicita todos os eventos de dispositivo do kernel após a

disponibilização do sistema de arquivos raiz, assim basta executar novamente o evento para o dispositivo de mouse USB. Então ele encontra o módulo de kernel no sistema de arquivos raiz montado e o mouse USB pode ser inicializado.

No espaço do usuário, não há diferença visível entre uma sequência coldplug do dispositivo e uma detecção de dispositivo durante a execução. Em ambos os casos, as mesmas regras são usadas para correspondência e os mesmos programas configurados são executados.

16.5 Monitorando o daemon `udev` em execução

O programa `udevadm monitor` pode ser usado para visualizar os eventos centrais do driver e a temporização dos processos de eventos do udev.

```
UEVENT[1185238505.276660] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UDEV  [1185238505.279198] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UEVENT[1185238505.279527] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV  [1185238505.285573] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UDEV  [1185238505.305026] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UEVENT[1185238505.305442] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
UEVENT[1185238505.306440] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.325384] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV  [1185238505.342257] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
```

As linhas `UEVENT` mostram os eventos que o kernel enviou através de netlink. As linhas `UDEV` mostram os handlers de evento do udev concluídos. A temporização é impressa em microssegundos. O tempo entre `UEVENT` e `UDEV` é o tempo que udev levou para processar esse evento ou que o daemon udev atrasou sua execução para sincronizar esse evento com eventos relacionados e já em execução. Por exemplo, eventos para partições de disco rígido sempre esperam pela conclusão do evento do

dispositivo de disco principal, pois os eventos de partição podem se basear nos dados que o evento de disco principal consultou do hardware.

`udevadm monitor --env` mostra o ambiente de evento completo:

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

O `udev` também envia mensagens para o syslog. A prioridade syslog padrão que controla as mensagens que são enviadas ao syslog é especificada no arquivo de configuração do `udev` `/etc/udev/udev.conf`. A prioridade de registro do daemon em execução pode ser modificada com `udevcontrol log_priority=`*`level/number`*.

16.6 Influenciando o gerenciamento de eventos de dispositivo do Kernel com as regras do `udev`

Uma regra do `udev` pode corresponder a qualquer propriedade que o kernel adiciona ao evento propriamente dito ou a qualquer informação que o kernel exporta para `sysfs`. A regra também pode solicitar informações adicionais de programas externos. Cada evento é correspondido com as regras fornecidas. Essas regras estão localizadas no diretório `/etc/udev/rules.d`.

Cada linha no arquivo de regras contém pelo menos um par de valores de chave. Há dois tipos de chaves, de atribuição e correspondência. Se todas as chaves de correspondência corresponderem aos valores, a regra será aplicada e as chaves de atribuição serão atribuídas ao valor especificado. Uma regra correspondente pode especificar o nome do nó de dispositivo, adicionar symlinks apontando para o nó ou executar um programa especificado como parte do tratamento de eventos. Se nenhuma

regra de correspondência for encontrada, o nome do nó de dispositivo padrão será usado para criar o nó de dispositivo. As informações detalhadas sobre a sintaxe da regra e as chaves fornecidas para corresponder ou importar os dados estão descritas na página de manual do udev. As regras de exemplo a seguir apresentam uma introdução básica à sintaxe da regra do udev. As regras de exemplo foram todas tiradas do conjunto de regras padrão do udev localizado em /etc/udev/rules.d/50-udev-default.rules.

Exemplo 16.1 *Regras do udev de exemplo*

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

A regra do console consiste em três chaves: uma chave de correspondência (KERNEL) e duas chaves de atribuição (MODE, OPTIONS). A regra de correspondência KERNEL pesquisa qualquer item do tipo console na lista de dispositivos. Apenas correspondências exatas são válidas e acionam essa regra para que seja executada. A chave MODE atribui permissões especiais ao nó de dispositivo, neste caso, permissões de leitura e gravação apenas ao proprietário desse dispositivo. A chave OPTIONS torna esta a última regra a ser aplicada a qualquer dispositivo desse tipo. Qualquer regra posterior que corresponda a esse tipo de dispositivo em particular não terá nenhum efeito.

A regra dos dispositivos seriais não está mais disponível em 50-udev-default.rules, mas ainda vale a pena ser considerada. Consiste em duas chaves de correspondência (KERNEL e ATTRS) e uma de atribuição (SYMLINK). A chave KERNEL procura todos os dispositivos do tipo ttyUSB. Usando o curinga *, essa chave corresponde a diversos desses dispositivos. A segunda chave de correspondência, ATTRS, verifica se o arquivo de atribuição do produto em sysfs para qualquer dispositivo ttyUSB contém uma determinada string. A chave de atribuição (SYMLINK) aciona a adição de um link simbólico para esse dispositivo em /dev/pilot. O operador usado nessa chave (+=) diz ao udev para executar essa ação adicionalmente, mesmo se regras anteriores ou posteriores adicionarem outros links simbólicos. Como

essa regra contém duas chaves de correspondência, ela é aplicada apenas se ambas as condições são cumpridas.

A regra da impressora lida com impressoras USB e contém duas chaves de correspondência que devem ser aplicadas para que a regra inteira seja aplicada (SUBSYSTEM e KERNEL). Três chaves de atribuição lidam com a nomeação desse tipo de dispositivo (NAME), a criação dos links de dispositivo simbólicos (SYMLINK) e a participação no grupo desse tipo de dispositivo (GROUP). O uso do curinga * na chave KERNEL faz com que ela corresponda a diversos dispositivos de impressora lp. Substituições são usadas pelo nome do dispositivo interno tanto na chave NAME quanto na SYMLINK para estender essas strings. Por exemplo, o symlink para a primeira impressora USB lp seria lido como /dev/usblp0.

A regra do carregador de firmware do kernel faz o udev carregar firmware adicional por um script de assistente externo durante o tempo de execução. A chave de correspondência SUBSYSTEM procura o subsistema de firmware. A chave ACTION verifica se algum dispositivo pertencente ao subsistema de firmware foi adicionado. A chave RUN+= aciona a execução do script firmware.sh para localizar o firmware a ser carregado.

Algumas características são comuns a todas as regras:

- Cada regra é composta por um ou mais pares de valores de chaves separados por vírgula.
- A operação de uma chave é determinada pelo operador. As regras do udev suportam diversos operadores diferentes.
- Cada valor dado deve estar entre aspas.
- Cada linha do arquivo de regras representa uma regra. Se uma regra for mais extensa e não couber em uma linha, use \ para juntar as linhas diferentes como se faria na sintaxe do shell.
- As regras do udev suportam um padrão no estilo do shell que corresponde aos padrões de *, ? e [].
- As regras do udev suportam substituições.

16.6.1 Usando operadores nas regras do `udev`

Ao criar chaves, você pode escolher dentre diversos operadores diferentes, dependendo do tipo de chave que quiser criar. As chaves de correspondência normalmente são usadas apenas para encontrar um valor que corresponda ou que explicitamente não corresponda ao valor de pesquisa. As chaves de correspondência contêm um dos seguintes operadores:

`==`
: Comparar para igualdade. Se a chave contém um padrão de pesquisa, todos os resultados correspondentes a esse padrão são válidos.

`!=`
: Comparar para não igualdade. Se a chave contém um padrão de pesquisa, todos os resultados correspondentes a esse padrão são válidos.

Qualquer um dos operadores a seguir também pode ser usado com chaves de atribuição:

`=`
: Atribuir um valor a uma chave. Se a chave consistia anteriormente em uma lista de valores, ela é redefinida e apenas o valor único é atribuído.

`+=`
: Adicionar um valor a uma chave que contenha uma lista de entradas.

`:=`
: Atribuir um valor final. Não permitir nenhuma mudança posterior por regras posteriores.

16.6.2 Usando substituições nas regras do `udev`

As regras do `udev` suportam o uso de marcadores e substituições. Use-as como faria em qualquer outro script. É possível usar as seguintes substituições com as regras do `udev`:

`%r`, `$root`
: O diretório do dispositivo, `/dev` por padrão.

`%p`, `$devpath`
: O valor de `DEVPATH`.

`%k`, `$kernel`
: O valor de `KERNEL` ou o nome do dispositivo interno.

`%n`, `$number`
: O nome do dispositivo.

`%N`, `$tempnode`
: O nome temporário do arquivo de dispositivo.

`%M`, `$major`
: O número maior do dispositivo.

`%m`, `$minor`
: O número menor do dispositivo.

`%s{`*`attribute`*`}`, `$attr{`*`attribute`*`}`
: O valor de um atributo `sysfs` (especificado por *`attribute`*).

`%E{`*`variable`*`}`, `$attr{`*`variable`*`}`
: O valor de uma variável do ambiente (especificado por *`variable`*).

`%c`, `$result`
: A saída de `PROGRAM`.

`%%`
: O caractere `%`.

`$$`
: O caractere `$`.

16.6.3 Usando as chaves de correspondência do udev

As chaves de correspondência descrevem as condições que devem ser atendidas para aplicar uma regra do `udev`. As seguintes chaves de correspondência estão disponíveis:

`ACTION`
: O nome da ação do evento, por exemplo, `add` ou `remove` na adição ou remoção de um dispositivo.

`DEVPATH`
: O caminho do dispositivo do evento, por exemplo, `DEVPATH=/bus/pci/drivers/ipw3945` para procurar todos os eventos relacionados ao driver ipw3945.

`KERNEL`
: O nome interno (do kernel) do dispositivo do evento.

`SUBSYSTEM`
: O subsistema do dispositivo do evento, por exemplo, `SUBSYSTEM=usb` para todos os eventos relacionados a dispositivos USB.

`ATTR{`*`nome de arquivo`*`}`
: Atributos `sysfs` do dispositivo do evento. Para corresponder a uma string contida no nome de arquivo do atributo `vendor`, você poderia usar `ATTR{vendor}=="On[sS]tream"`, por exemplo.

`KERNELS`
: Permitem que o `udev` pesquise o caminho do dispositivo para encontrar um nome de dispositivo correspondente.

`SUBSYSTEMS`
: Permitem que o `udev` pesquise o caminho do dispositivo para encontrar um nome de subsistema do dispositivo correspondente.

`DRIVERS`
: Permitem que o `udev` pesquise o caminho do dispositivo para encontrar um nome de driver do dispositivo correspondente.

`ATTRS{`*`nome de arquivo`*`}`
: Permitem que o `udev` pesquise o caminho do dispositivo para encontrar um com valores de atributo `sysfs` correspondentes.

`ENV{`*`chave`*`}`
: O valor de uma variável de ambiente, por exemplo, `ENV{ID_BUS}="ieee1394` para procurar todos os eventos relacionados ao ID do barramento FireWire.

`PROGRAM`
: Permite que o `udev` execute um programa externo. Para ser bem-sucedido, o programa deve retornar com código de saída zero. A saída do programa, impressa em stdout, está disponível para a chave `RESULT`.

`RESULT`
: Corresponder à string de saída da última chamada de `PROGRAM`. Incluir esta chave na mesma regra que a chave `PROGRAM` ou em uma posterior.

16.6.4 Usando as chaves de atribuição do udev

Em contraste com as chaves de correspondência descritas anteriormente, as chaves de atribuição não descrevem condições que devem ser cumpridas. Elas atribuem valores, nomes e ações aos nós do dispositivo mantidos pelo `udev`.

`NAME`
: O nome do nó de dispositivo a ser criado. Após uma regra definir um nome de nó, todas as demais regras com uma chave `NAME` para esse nó são ignoradas.

`SYMLINK`
: O nome de um symlink relacionado a um nó a ser criado. Várias regras de correspondência podem adicionar symlinks a serem criados com o nó de dispositivo. Você também pode especificar vários symlinks para um nó em uma regra usando o caractere de espaço para separar os nomes dos symlinks.

`OWNER, GROUP, MODE`
: As permissões do novo nó de dispositivo. Os valores especificados aqui sobregravam qualquer coisa que tenha sido compilada.

`ATTR{chave}`
: Especifica um valor para ser gravado no atributo `sysfs` do dispositivo de evento. Se o operador == é usado, essa chave também é usada para corresponder com o valor de um atributo sysfs.

`ENV{chave}`
: Indica ao `udev` para exportar uma variável para o ambiente. Se o operador == é usado, essa chave também é usada para corresponder com uma variável de ambiente.

`RUN`
: Indica ao `udev` para adicionar um programa à lista de programas a serem executados neste dispositivo. Lembre-se de restringir isso a tarefas muito curtas, a fim de evitar o bloqueio de outros eventos para esse dispositivo.

`LABEL`
: Adicionar um rótulo para onde um `GOTO` possa ir.

`GOTO`
: Indica ao `udev` para ignorar uma quantidade de regras e continuar com uma que inclua o rótulo citado pela chave `GOTO`.

`IMPORT{tipo}`
: Carregar variáveis para o ambiente do evento, como a saída de um programa externo. O `udev` importa variáveis de vários tipos diferentes. Se nenhum tipo for especificado, o `udev` tentará determinar o tipo sozinho, com base na parte executável das permissões do arquivo.

  - `program` diz ao `udev` para executar um programa externo e importar sua saída.
  - `file` diz ao `udev` para importar um arquivo texto.
  - `parent` diz ao `udev` para importar as chaves armazenadas do dispositivo pai.

`WAIT_FOR_SYSFS`
: Indica ao `udev` para aguardar a criação do arquivo `sysfs` especificado para determinado dispositivo. Por exemplo, `WAIT_FOR_SYSFS="ioerr_cnt"` informa o udev para aguardar até que o arquivo `ioerr_cnt` seja criado.

OPTIONS
A chave OPTION pode ter diversos valores possíveis:

- last_rule diz ao udev para ignorar todas as regras posteriores.
- ignore_device diz ao udev para ignorar esse evento completamente.
- ignore_remove diz ao udev para ignorar todos os eventos de remoção posteriores para o dispositivo.
- all_partitions diz ao udev para criar nós de dispositivo para todas as partições disponíveis em um dispositivo de bloco.

16.7 Nomeação de dispositivo persistente

O diretório do dispositivo dinâmico e a infraestrutura de regras do udev possibilitam especificar nomes estáveis para todos os dispositivos de disco, independentemente da ordem de reconhecimento ou da conexão usada para o dispositivo. Cada dispositivo de bloco apropriado criado pelo kernel é examinado por ferramentas com conhecimento especial sobre determinados barramentos, tipos de unidade ou sistemas de arquivos. Com o nome do nó do dispositivo fornecido pelo kernel dinâmico, o udev mantém as classes de links persistentes apontando para o dispositivo:

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
|   |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
|   `-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
|   |-- Photos -> ../../sdd1
|   |-- SUSE10 -> ../../sda7
|   `-- devel -> ../../sda6
|-- by-path
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
|   |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
```

```
|   |-- usb-02773:0:0:2 -> ../../sdd
|   |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    `-- 4210-8F8C -> ../../sdd1
```

16.8 Arquivos usados pelo `udev`

`/sys/*`
: Sistema de arquivos virtual fornecido pelo kernel do Linux, exportando todos os dispositivos conhecidos atualmente. Essas informações são usadas pelo `udev` para criar nós de dispositivo em `/dev`

`/dev/*`
: Nós de dispositivo criados dinamicamente e conteúdo estático copiados no momento do boot de `/lib/udev/devices/*`

Os arquivos e os diretórios a seguir incluem elementos cruciais da infraestrutura do `udev`:

`/etc/udev/udev.conf`
: Arquivo de configuração principal do `udev`.

`/etc/udev/rules.d/*`
: Regras de correspondência de evento do `udev`.

`/lib/udev/devices/*`
: Conteúdo `/dev` estático.

`/lib/udev/*`
: Programas ajudantes chamados de regras do `udev`.

16.9 Para obter mais informações

Para obter mais informações sobre a infraestrutura do `udev`, consulte as seguintes páginas de manual:

`udev`
: Informações importantes sobre `udev`, chaves, regras e outras questões essenciais de configuração.

`udevadm`
: É possível usar o `udevadm` para controlar o comportamento de tempo de execução do `udev`, solicitar eventos do kernel, gerenciar a fila de eventos e fornecer mecanismos simples de depuração.

`udevd`
: Informações sobre o daemon de gerenciamento de eventos do `udev`.

O sistema X Window 17

O sistema X Window (X11) é o padrão de fato para interfaces gráficas de usuário no UNIX. O X é baseado em rede, permitindo que aplicativos iniciados em um host sejam exibidos em outro host conectado em qualquer tipo de rede (LAN ou Internet). Este capítulo descreve a configuração e otimização do ambiente do X Window System e apresenta informações sobre o uso das fontes no SUSE® Linux Enterprise Desktop.

17.1 Configurando manualmente o sistema X Window

Por padrão, o X Window System é configurado com a interface do SaX2, descrita no Section “Setting Up Graphics Card and Monitor” (Chapter 5, *Setting Up Hardware Components with YaST*, ↑*Deployment Guide*). Alternativamente, pode ser configurado manualmente, editando seus arquivos de configuração.

ATENÇÃO: configurações defeituosas do X podem danificar seu hardware

Tenha cuidado ao configurar o sistema X Window. Nunca inicie o sistema X Window antes que a configuração esteja concluída. Um sistema mal configurado pode causar danos irreparáveis ao seu hardware (isso se aplica particularmente a monitores de frequência fixa). Os autores deste manual e do SUSE Linux Enterprise Desktop não podem ser responsabilizados por nenhum dano resultante. Essas informações foram pesquisadas cuidadosamente, mas isso não garante que todos os métodos apresentados aqui estejam corretos e não danifiquem o seu hardware.

O comando `sax2` cria o arquivo `/etc/X11/xorg.conf`. Esse é o arquivo de configuração principal do Sistema X Window. A seguir estão todas as configurações referentes ao monitor, ao mouse e à placa de vídeo.

IMPORTANTE: usando o X -configure

Use o `X -configure` para definir a configuração do X se houver falha nas tentativas anteriores com o SaX2 do SUSE Linux Enterprise Desktop. Se sua configuração envolve drivers proprietários apenas binários, o `X -configure` não funcionará.

As seções a seguir descrevem a estrutura do arquivo de configuração `/etc/X11/xorg.conf`. Ela consiste em várias seções, cada uma delas referente a um determinado aspecto da configuração. Cada seção se inicia com a palavra-chave `Section <designation>` e termina com `EndSection`. A convenção a seguir se aplica a todas as seções:

```
Section "designation"
  entry 1
  entry 2
  entry n
EndSection
```

Os tipos de seção disponíveis estão listados na Tabela 17.1, “Seções em /etc/X11/xorg.conf” (p 226).

Tabela 17.1 *Seções em /etc/X11/xorg.conf*

Tipo	Significado
`Files`	Os caminhos usados para as fontes e a tabela de cores RGB.
`ServerFlags`	Switches gerais para o comportamento do servidor.
`Module`	Uma lista de módulos que o servidor deve carregar
`InputDevice`	Dispositivos de entrada, como teclados e dispositivos de entrada especiais

Tipo	Significado
	(touchpads, joysticks, etc.), são configurados nessa seção. Parâmetros importantes nessa seção são `Driver` e as opções que definem o `Protocol` e o `Device`. Você normalmente tem uma seção `InputDevice` por dispositivo conectado ao computador.
`Monitor`	O monitor usado. Elementos importantes dessa seção são o `Identifier`, mencionado posteriormente na definição de `Screen`, a taxa de atualização `VertRefresh` e os limites da frequência de sincronização (`HorizSync` e `VertRefresh`). As configurações são fornecidas em MHz, kHz e Hz. Normalmente, o servidor recusa qualquer linha modelo que não corresponda à especificação do monitor. Isso evita que frequências muito altas sejam enviadas ao monitor por acidente.
`Modes`	Os parâmetros de modeline para as resoluções de tela específicas. Esses parâmetros podem ser calculados por SaX2 com base nos valores fornecidos pelo usuário e, normalmente, não precisam ser modificados. Intervenha manualmente nesse ponto se, por exemplo, quiser conectar um monitor de frequência fixa. Há detalhes sobre o significado dos valores numéricos individuais nos arquivos HOWTO, em `/usr/share/doc/howto/en/`

Tipo	Significado
	html/XFree86-Video-Timings-HOWTO (disponíveis no pacote howtoenh). Para calcular os modos VESA manualmente, você pode usar a ferramenta cvt. Por exemplo, para calcular uma modeline para um monitor de 1680x1050 a 60 Hz, use o comando cvt 1680 1050 60.
Device	Uma placa de vídeo específica. Ela é referenciada por seu nome descritivo. As opções disponíveis nessa seção dependem muito do driver usado. Por exemplo, se você usa o driver i810, encontre mais informações sobre as opções disponíveis na página de manual man 4 i810.
Screen	Combina um Monitor e um Device para formar todas as configurações necessárias para o X.Org. Na subseção Display, especifique o tamanho da tela virtual (Virtual), a ViewPort e os Modes usados com essa tela. Note que alguns drivers exigem que todas as configurações usadas estejam presentes na seção Display em algum lugar. Por exemplo, se você usa um laptop e deseja usar um monitor externo que seja maior do que o LCD interno, pode ser necessário adicionar uma resolução maior do que a suportada pelo LCD interno ao final da linha Modes.

Tipo	Significado
ServerLayout	O layout de uma configuração single-thread ou multithread. Essa seção junta os dispositivos de entrada InputDevice e os dispositivos de exibição Screen.
DRI	Fornece informações para a Infraestrutura de Renderização Direta (DRI).

Monitor, Device e Screen são explicados em mais detalhes. Mais informações sobre as outras seções podem ser encontradas nas páginas de manual de X.Org e xorg .conf.

Há várias seções Monitor e Device diferentes em xorg.conf. Mesmo várias seções Screen são possíveis. A seção ServerLayout determina qual dessas seções é usada.

17.1.1 Seção de tela

A seção de tela combina um monitor com uma seção de dispositivo e determina a resolução e a intensidade de cor usadas. Uma seção de tela pode ter a aparência do Exemplo 17.1, "Seção de tela do arquivo /etc/X11/xorg.conf" (p 229).

Exemplo 17.1 *Seção de tela do arquivo /etc/X11/xorg.conf*

```
Section "Screen"❶
  DefaultDepth  16❷
  SubSection "Display"❸
    Depth       16❹
    Modes       "1152x864" "1024x768" "800x600"❺
    Virtual     1152x864❻
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
```

```
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"❼
  Monitor       "Monitor[0]"
EndSection
```

❶ `Section` determina o tipo de seção, neste caso, `Screen`.

❷ `DefaultDepth` determina a profundidade de cores a ser usada por padrão, a menos que outra seja especificada explicitamente.

❸ Para cada profundidade de cores, diferentes subseções `Display` são especificadas.

❹ `Depth` determina a profundidade de cores a ser usada com esse conjunto de configurações de `Display`. Os valores possíveis são `8`, `15`, `16`, `24` e `32`, embora nem todos sejam suportados por todos os módulos do servidor X ou resoluções.

❺ A seção `Modes` apresenta uma lista de possíveis resoluções de tela. O servidor X verifica essa lista da esquerda para a direita. Para cada resolução, o servidor X procura uma `Modeline` adequada na seção `Modes`. A `Modeline` depende da capacidade do monitor e da placa de vídeo. As configurações de `Monitor` determinam a `Modeline` resultante.

A primeira resolução encontrada é o `Default mode`. Com Ctrl + Alt + + (no teclado numérico), alterne para a resolução seguinte na lista à direita. Com Ctrl + Alt + – (no teclado numérico), alterne para a anterior. Isso permite a você variar a resolução enquanto o X está sendo executado.

❻ A última linha da subseção `Display` com `Depth 16` refere-se ao tamanho da tela virtual. O tamanho máximo possível de uma tela virtual depende da quantidade de memória instalada na placa de vídeo e da intensidade de cor desejada, não da resolução máxima do monitor. Se essa linha é omitida, a resolução virtual é apenas a resolução física. Como placas de vídeo modernas têm uma grande quantidade de memória de vídeo, você pode criar áreas de trabalho virtuais bem grandes. Porém, você talvez não possa mais usar a funcionalidade de 3D se preencher a maior parte da memória de vídeo com uma área de trabalho virtual. Por exemplo, se a placa tiver 16 MB de memória RAM de vídeo, a tela virtual poderá ter até 4096x4096 pixels de tamanho, com profundidade de cores de 8 bits. Porém, principalmente para placas aceleradas, não é recomendável usar toda a memória para a tela virtual, pois a memória da placa também é usada para vários caches de vídeo e fontes.

❼ A linha Identifier (aqui Screen[0]) fornece a essa seção um nome definido com o qual ela pode ser referenciada com exclusividade na seguinte seção ServerLayout. As linhas Device e Monitor especificam a placa de vídeo e o monitor que pertencem a essa definição. Esses são links para as seções Device e Monitor com seus nomes correspondentes ou *identificadores*. Essas seções são abordadas em detalhes abaixo.

17.1.2 Seção do dispositivo

Uma seção de dispositivo descreve uma placa de vídeo específica. Você pode ter quantas entradas de dispositivo desejar em xorg.conf, desde que os nomes sejam diferenciados pela palavra-chave Identifier. Se você tiver mais de uma placa de vídeo instalada, as seções serão simplesmente numeradas em ordem. A primeira é chamada Device[0], a segunda Device[1] e assim por diante. O arquivo a seguir mostra um trecho da seção Device de um computador com uma placa de vídeo Matrox Millennium PCI (conforme configurada pelo SaX2):

```
Section "Device"
  BoardName      "MGA2064W"
  BusID          "0:19:0"❶
  Driver         "mga"❷
  Identifier     "Device[0]"
  VendorName     "Matrox"
  Option         "sw_cursor"
EndSection
```

❶ O BusID refere-se ao slot PCI ou AGP no qual a placa de vídeo está instalada. Isso corresponde ao ID exibido pelo comando lspci. O servidor X precisa de detalhes no formato decimal, mas o lspci os exibe no formato hexadecimal. O valor de BusID é detectado automaticamente pelo SaX2.

❷ O valor de Driver é definido automaticamente pelo SaX2 e especifica qual o driver a ser usado para a sua placa de vídeo. Se a placa for Matrox Millennium, o módulo do driver será chamado mga. Em seguida, o servidor X pesquisa no ModulePath definido na seção Files no subdiretório drivers. Em uma instalação padrão, é o diretório /usr/lib/xorg/modules/drivers ou o /usr/lib64/xorg/modules/drivers para o diretório de sistemas operacionais de 64 bits. _drv.o será adicionado ao nome, por isso, no caso do driver mga, o arquivo de driver mga_drv.o será carregado.

O comportamento do servidor X ou do driver também pode ser influenciado por meio de opções adicionais. Um exemplo disso é a opção `sw_cursor`, definida na seção de dispositivo. Isso desativa o cursor do mouse do hardware e mostra o cursor do mouse usando o software. Dependendo do módulo do driver, há várias opções disponíveis (que podem ser encontradas nos arquivos de descrição dos módulos do driver no diretório `/usr/share/doc/packages/`*`nome_do_pacote`*). Opções geralmente válidas também podem ser encontradas nas páginas de manual (`man xorg.conf`, `man 4` *`<driver module>`* e `man 4` *`chips`*).

Se a placa de vídeo tem vários conectores de vídeo, é possível configurar os diferentes dispositivos dessa placa como uma única tela. Use o SaX2 para configurar a interface de vídeo dessa maneira.

17.1.3 Seção Monitor e Modes

Como as seções `Device`, as seções `Monitor` e `Modes` descrevem um monitor cada. O arquivo de configuração `/etc/X11/xorg.conf` pode conter quantas seções `Monitor` você desejar. Cada seção `Monitor` faz referência a uma seção `Modes` com a linha `UseModes`, se houver. Se não houver nenhuma seção `Modes` disponível para a seção `Monitor`, o servidor X calculará valores apropriados a partir dos valores de sincronização gerais. A seção de layout do servidor especifica qual seção `Monitor` é relevante.

Definições de monitor devem ser configuradas por usuários experientes. As modelines constituem uma parte importante das seções `Monitor`. Linhas modelo definem temporizações verticais para a respectiva resolução. As propriedades do monitor, especialmente as frequências permitidas, estão armazenadas na seção `Monitor.` Modos VESA padrão podem ser gerados com o utilitário `cvt`. Para obter mais informações, leia a página de manual do cvt `man cvt`.

ATENÇÃO

A menos que você tenha conhecimento aprofundado sobre as funções do monitor e da placa de vídeo, não mude as modelines, pois isso pode danificar gravemente o monitor.

As pessoas que tentam desenvolver suas próprias descrições de monitor devem estar familiarizadas com a documentação em /usr/share/X11/doc. Instale o pacote xorg-x11-doc para encontrar PDFs e páginas em HTML.

A especificação manual de linhas modelo raramente é exigida atualmente. Se você está usando um monitor multisync moderno, as frequências permitidas e as resoluções ótimas podem, como regra, serem lidas do monitor pelo servidor X através de DDC, como descrito na seção de configuração do SaX2. Se isso não for possível por algum motivo, use um dos modos VESA incluídos no servidor X. Isso funcionará com a maioria das combinações de monitor e placa de vídeo.

17.2 Instalando e configurando fontes

A instalação de fontes adicionais no SUSE Linux Enterprise Desktop é muito fácil. Simplesmente copie as fontes para qualquer diretório localizado no caminho da fonte X11 (consulte a Seção 17.2.1, “Fontes centrais X11” (p 234)). Para habilitar o uso das fontes, o diretório de instalação deve ser um subdiretório dos diretórios configurados em /etc/fonts/fonts.conf (consulte a Seção 17.2.2, “Xft” (p 235)) ou inclusos neste arquivo com /etc/fonts/suse-font-dirs.conf.

O arquivo a seguir é um exemplo de /etc/fonts/fonts.conf. Esse é o arquivo de configuração padrão que deve ser apropriado para a maioria das configurações. Define também o diretório incluso /etc/fonts/conf.d. Nesse diretório, todos os arquivos ou links simbólicos que começam com um número de dois dígitos são carregados pelo fontconfig. Para obter uma explicação mais detalhada dessa funcionalidade, consulte /etc/fonts/conf.d/README.

```
<!-- Font directory list -->
<dir>/usr/share/fonts</dir>
<dir>/usr/X11R6/lib/X11/fonts</dir>
<dir>/opt/kde3/share/fonts</dir>
<dir>/usr/local/share/fonts</dir>
<dir>~/.fonts</dir>
```

/etc/fonts/suse-font-dirs.conf é gerado automaticamente para extrair fontes que acompanham aplicativos (em sua maioria, de terceiros) como LibreOffice, Java ou Adobe Reader. Uma entrada típica seria semelhante ao seguinte:

```
<dir>/usr/lib/Adobe/Reader9/Resource/Font</dir>
<dir>/usr/lib/Adobe/Reader9/Resource/Font/PFM</dir>
```

Para instalar outras fontes em todo o sistema, copie manualmente os arquivos de fontes para o diretório adequado (como `root`); por exemplo, `/usr/share/fonts/truetype`. Alternativamente, a tarefa pode ser realizada com o instalador de fontes do KDE no Centro de Controle do KDE. O resultado é o mesmo.

Em vez de copiar as fontes reais, você também pode criar links simbólicos. Por exemplo, é recomendável fazer isso se você tiver fontes licenciadas em uma partição do Windows montada e desejar usá-las. Em seguida, execute `SuSEconfig --module fonts` .

`SuSEconfig --module fonts` executa o script `/usr/sbin/fonts-config`, que lida com a configuração das fontes. Para obter mais informações sobre esse script, consulte sua página de manual (`man fonts-config`).

O procedimento é o mesmo para fontes de bitmap, fontes TrueType e OpenType, e fontes Type1 (PostScript). Todos esses tipos de fonte podem ser instalados em qualquer diretório.

O X.Org contém dois sistemas de fontes completamente diferentes: o antigo *sistema de fontes centrais X11* e o recém-criado sistema *Xft e fontconfig*. As seções a seguir descrevem brevemente esses dois sistemas.

17.2.1 Fontes centrais X11

Atualmente, o sistema de fontes centrais X11 suporta não apenas fontes de bitmap, mas também fontes escaláveis, como fontes Type1, TrueType e OpenType. Fontes escaláveis só são suportadas sem suavização e renderização de subpixel, e o carregamento de fontes escaláveis grandes com glifos para muitos idiomas pode levar bastante tempo. As fontes Unicode também são suportadas, mas seu uso pode ser lento e exigir mais memória.

O sistema de fontes centrais X11 tem algumas fraquezas inerentes. Ele está desatualizado e não pode mais ser estendido de forma significativa. Embora ele possa ser mantido por motivos de compatibilidade retroativa, o sistema Xft e fontconfig mais moderno deve ser usado se for possível.

Para sua operação, o servidor X precisa saber quais fontes estão disponíveis e onde ele pode encontrá-las no sistema. Isso é tratado por uma variável `FontPath`, que contém o caminho para todos os diretórios de fontes de sistemas válidos. Em cada um desses

diretórios, um arquivo chamado fonts.dir lista as fontes disponíveis nesse diretório. O FontPath é gerado pelo servidor X na inicialização. Ele procura um arquivo fonts.dir válido em cada uma das entradas FontPath no arquivo de configuração /etc/X11/xorg.conf. Essas entradas são encontradas na seção Files. Exiba o FontPath real com xset q. Esse caminho também pode ser modificado no tempo de execução com xset. Para adicionar outro caminho, use xset +fp <caminho>. Para remover um caminho indesejado, use xset -fp <caminho>.

Se o servidor X já estiver ativo, fontes recém-instaladas em diretórios montados poderão ser disponibilizadas com o comando xsetfp rehash. Esse comando é executado por SuSEconfig --module fonts. Como o comando xset precisa de acesso ao servidor X em execução, isso funciona apenas se SuSEconfig --module fonts for iniciado de um shell com acesso ao servidor X em execução. A maneira mais fácil de conseguir isso é adquirir permissões de root digitando su e a senha de root. su transfere as permissões de acesso do usuário que iniciou o servidor X para o shell do root. Para verificar se as fontes foram instaladas corretamente e estão disponíveis por meio do sistema de fontes centrais X11, use o comando xlsfonts para listar todas as fontes disponíveis.

Por padrão, o SUSE Linux Enterprise Desktop usa idiomas UTF-8. Dessa forma, fontes Unicode devem ser preferidas (nomes de fontes terminados com iso10646-1 na saída xlsfonts). Todas as fontes Unicode disponíveis podem ser relacionadas com xlsfonts | grep iso10646-1. Praticamente todas as fontes Unicode disponíveis no SUSE Linux Enterprise Desktop contêm pelo menos os glifos necessários para idiomas europeus (antes codificados como iso-8859-*).

17.2.2 Xft

Desde o início, os programadores do Xft verificaram se as fontes escaláveis com suavização eram bem suportadas. Se o Xft for usado, as fontes serão exibidas pelo aplicativo usando as fontes, não pelo servidor X como no sistema de fontes central X11. Dessa forma, o respectivo aplicativo tem acesso aos arquivos de fontes reais e controle total sobre como os glifos são exibidos. Isso constitui a base para a exibição correta do texto em vários idiomas. Acesso direto aos arquivos de fontes é bastante útil para embutir fontes para impressão para garantir que a impressão tenha a mesma aparência da saída da tela.

No SUSE Linux Enterprise Desktop, os dois ambientes de área de trabalho (KDE e GNOME), o Mozilla e vários outros aplicativos já usam o Xft por padrão. O Xft já é usado por mais aplicativos do que o sistema de fontes central X11 antigo.

O Xft usa a biblioteca fontconfig para localizar fontes e influenciar a maneira como elas são exibidas. As propriedades do fontconfig são controladas pelo arquivo de configuração global `/etc/fonts/fonts.conf`. Configurações especiais devem ser adicionadas a `/etc/fonts/local.conf` e ao arquivo de configuração específico do usuário `~/.fonts.conf`. Cada um desses arquivos de configuração fontconfig deve iniciar com

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

e terminar com

```
</fontconfig>
```

Para adicionar diretórios para pesquisar fontes, acrescente linhas como as seguintes:

```
<dir>/usr/local/share/fonts/</dir>
```

Porém, isso geralmente não é necessário. Por padrão, o diretório específico do usuário `~/.fonts` já está inserido em `/etc/fonts/fonts.conf`. Da mesma maneira, tudo o que você precisa fazer para instalar fontes adicionais é copiá-las para `~/.fonts`.

Você também pode inserir regras que influenciam a aparência das fontes. Por exemplo, digite

```
<match target="font">
 <edit name="antialias" mode="assign">
  <bool>false</bool>
 </edit>
</match>
```

para desabilitar a suavização de todas as fontes ou

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

para desabilitar a suavização de fontes específicas.

Por padrão, a maioria dos aplicativos usa os nomes de fontes `sans-serif` (ou o equivalente `sans`), `serif` ou `monospace`. Essas não são fontes reais, mas somente aliás que são resolvidos para uma fonte adequada, dependendo da configuração de idioma.

Usuários podem facilmente adicionar regras para `~/.fonts.conf` a fim de resolver esses aliás para suas fontes favoritas:

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Como quase todos os aplicativos usam esses aliás por padrão, isso afeta praticamente todo o sistema. Dessa forma, você pode facilmente usar suas fontes favoritas praticamente em qualquer local, sem precisar modificar as configurações de fontes nos aplicativos individuais.

Use o comando `fc-list` para encontrar as fontes instaladas e disponíveis para uso. Por exemplo, o comando `fc-list` retorna uma lista de todas as fontes. Para descobrir quais das fontes escaláveis disponíveis (`:scalable=true`) contêm todos os glifos exigidos para hebraico (`:lang=he`), os nomes de fontes (`family`), o estilo (`style`), o peso (`weight`) e o nome dos arquivos que contêm as fontes, digite o seguinte comando:

```
fc-list ":lang=he:scalable=true" family style weight
```

A saída do comando pode ter a seguinte aparência:

```
Lucida Sans:style=Demibold:weight=200
DejaVu Sans:style=Bold Oblique:weight=200
Lucida Sans Typewriter:style=Bold:weight=200
DejaVu Sans:style=Oblique:weight=80
Lucida Sans Typewriter:style=Regular:weight=80
DejaVu Sans:style=Book:weight=80
DejaVu Sans:style=Bold:weight=200
Lucida Sans:style=Regular:weight=80
```

Parâmetros importantes podem ser consultados com `fc-list`:

Tabela 17.2 *Parâmetros de fc-list*

Parâmetro	Significado e valores possíveis
`family`	Nome da família da fonte, por exemplo, `FreeSans`.
`foundry`	Nome do fabricante da fonte, por exemplo, `urw`.
`style`	O estilo da fonte, como `Medium`, `Regular`, `Bold`, `Italic` ou `Heavy`.
`lang`	O idioma que a fonte suporta, por exemplo, `de` para alemão, `ja` para japonês, `zh-TW` para chinês tradicional ou `zh-CN` para chinês simplificado.
`weight`	O peso da fonte, como `80` para normal ou `200` para negrito.
`slant`	A inclinação, geralmente `0` para nenhum e `100` para itálico.
`SETUP.ISS`	O nome do arquivo que contém a fonte.
`outline`	`true` para fontes de bordas ou `false` para outras fontes.

Parâmetro	Significado e valores possíveis
scalable	true para fontes escaláveis ou false para outras fontes.
bitmap	true para fontes de bitmap ou false para outras fontes.
pixelsize	Tamanho de fonte em pixels. Em conexão com a fc-list, essa opção só faz sentido para fontes de bitmap.

17.3 Para obter mais informações

Instale os pacotes xorg-x11-doc e howtoenh para obter informações mais aprofundadas sobre o X11. Mais informações sobre o desenvolvimento do X11 podem ser encontradas na home page do projeto, em http://www.x.org.

Muitos dos drivers fornecidos com o pacote xorg-x11-driver-video são descritos em detalhes em uma página de manual. Por exemplo, se você usar o driver nv, encontre mais informações sobre ele em man 4 nv.

Informações sobre drivers de terceiros devem estar disponíveis em /usr/share/doc/packages/<nome_do_pacote>. Por exemplo, a documentação de x11-video-nvidiaG01 está disponível em /usr/share/doc/packages/x11-video-nvidiaG01 após a instalação do pacote.

Acessando sistemas de arquivos com o FUSE

18

FUSE é o acrônimo de *file system in userspace* (sistema de arquivos no espaço do usuário). Isso significa que você pode configurar e montar um sistema de arquivos como um usuário sem privilégios. Normalmente, é necessário ser o `root` para executar essa tarefa. O FUSE, isoladamente, é um módulo de kernel. Combinado-o a plug-ins, você pode estender o FUSE para acessar quase todos os sistemas de arquivos, como conexões SSH remotas, imagens ISO e muito mais..

18.1 Configurando o FUSE

Antes de usar o FUSE, é necessário instalar o pacote `fuse`. Dependendo do sistema de arquivos que você deseja usar, serão necessários plug-ins adicionais, disponíveis em pacotes separados.

Em geral, não é necessário configurar o FUSE, basta usá-lo. Mas vale a pena criar um diretório com todos os pontos de montagem combinados. Por exemplo, você pode criar um diretório `~/mounts` e inserir nele subdiretórios para os diferentes sistemas de arquivo.

18.2 Plug-ins disponíveis do FUSE

O FUSE depende de plug-ins. A tabela a seguir lista os plug-ins comuns.

Tabela 18.1 Plug-ins disponíveis do FUSE

`fuseiso`	monta imagens de CD-ROM contendo sistemas de arquivos ISO9660
`ntfs-3g`	monta volumes NTFS (com suporte de leitura e gravação)
`sshfs`	cliente de sistema de arquivos com base no protocolo de transferência de arquivo SSH
`wdfs`	monta sistemas de arquivos WebDAV

18.3 Para obter mais informações

Consulte a home page `http://fuse.sourceforge.net` do FUSE para obter mais informações.

Parte III. Computadores móveis

Computação móvel com o Linux

19

A computação móvel é geralmente associada a laptops, PDAs e telefones celulares (e ao intercâmbio de dados entre esses aparelhos). Componentes de hardware móveis, como discos rígidos externos, unidades flash ou câmeras digitais, podem ser conectados a laptops ou sistemas de desktop. Vários componentes de software estão envolvidos em cenários de computação e alguns aplicativos são desenvolvidos para uso móvel.

19.1 Laptops

O hardware de laptops difere do hardware de um sistema de desktop normal. Isso se deve a critérios como permutabilidade, requisitos de espaço e consumo de energia, que devem ser levados em conta. Os fabricantes de hardware móvel desenvolveram interfaces padrão, como PCMCIA (Personal Computer Memory Card International Association), Mini PCI e Mini PCIe, que podem ser usadas para estender o hardware de laptops. Os padrões abrangem cartões de memória, placas de interface de rede, ISDN (bem como placas de modem) e discos rígidos externos.

DICA: SUSE Linux Enterprise Desktop e tablet PCs

O SUSE Linux Enterprise Desktop também suporta Tablet PCs. Os Tablet PCs incluem um touchpad/digitalizador que permite usar uma caneta digital, ou mesmo as pontas dos dedos, para editar dados diretamente na tela, em vez de usar mouse e teclado. Eles são instalados e configurados de forma semelhante a qualquer outro sistema. Para obter uma introdução detalhada sobre a instalação e configuração de Tablet PCs, consulte o Capítulo 22, *Usando Tablet PCs* (p 285).

19.1.1 Conservação de energia

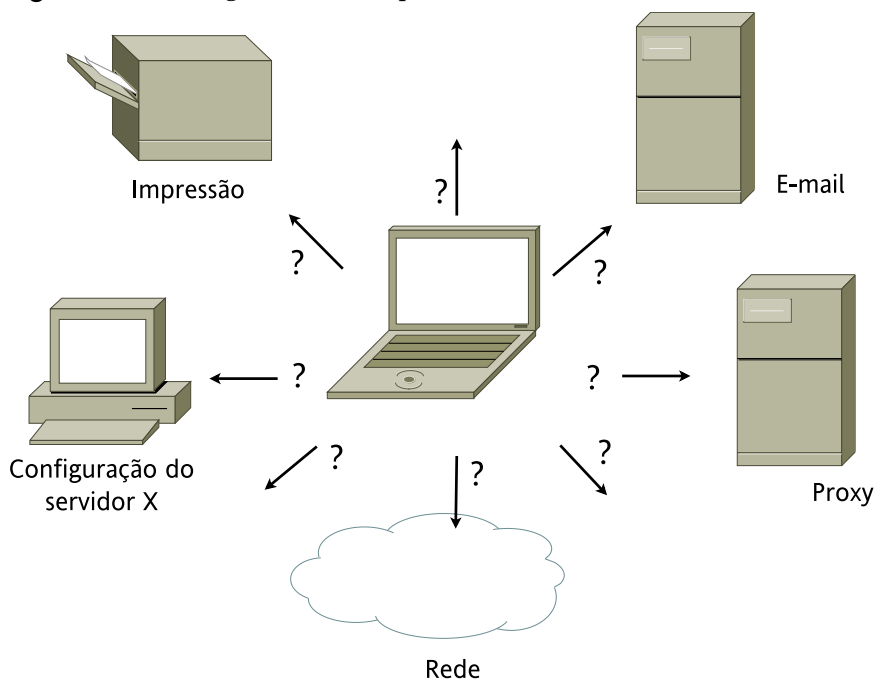
A inclusão de componentes de sistema com otimização de energia durante a fabricação de laptops contribui para a sua adequação ao uso sem acesso à rede elétrica. A contribuição desses componentes para a preservação de energia é, ao menos, tão importante quanto a do sistema operacional. O SUSE® Linux Enterprise Desktop suporta vários métodos que influenciam o consumo de energia de um laptop e possuem diversos efeitos sobre o tempo de operação durante o uso de energia da bateria. A lista a seguir está em ordem decrescente de contribuição para a conservação de energia:

- Regulagem da velocidade da CPU.
- Desativação da iluminação da tela durante pausas.
- Ajuste manual da iluminação da tela.
- Desconexão de acessórios não utilizados e habilitados para hotplug (CD-ROM USB, mouse externo, placas PCMCIA sem uso, WLAN etc.).
- Colocação do disco rígido em modo de espera quando inativo.

Você encontra informações detalhadas sobre o gerenciamento de energia do SUSE Linux Enterprise Desktop no Capítulo 21, *Gerenciamento de energia* (p 275). Para obter mais informações sobre gerenciamento de energia específico de área de trabalho, consulte a Seção “Controlando o gerenciamento de energia da área de trabalho” (Capítulo 2, *Trabalhando com a área de trabalho*, ↑*Guia do Usuário do GNOME*), que explica como usar o Gerenciador de Energia do GNOME. Mais informações sobre o applet de gerenciamento de energia do KDE estão disponíveis no Chapter 9, *Controlling Your Desktop's Power Management* (↑*KDE User Guide*).

19.1.2 Integração em ambientes operacionais variáveis

Seu sistema precisa se adaptar a ambientes operacionais variáveis quando for usado para a computação móvel. Vários serviços dependem do ambiente, e os clientes subjacentes precisam ser reconfigurados. O SUSE Linux Enterprise Desktop administra esta tarefa para você.

Figura 19.1 *Integrando um computador móvel em um ambiente existente*

Os serviços afetados no caso de um laptop que transita entre uma pequena rede doméstica e uma rede de escritório são:

Rede
: Inclui a atribuição de endereço IP, a resolução do nome, a conectividade à Internet e a conectividade a outras redes.

Impressão
: Precisam estar presentes um banco de dados atual de impressoras disponíveis e um servidor de impressão disponível, dependendo da rede.

E-mail e proxies
: Assim como ocorre com a impressão, a lista dos servidores correspondentes precisa ser atual.

X (ambiente gráfico)
: Se o seu laptop estiver temporariamente conectado a um projetor ou monitor externo, configurações de exibição diferentes precisam estar disponíveis.

O SUSE Linux Enterprise Desktop oferece várias maneiras de integrar laptops a ambientes operacionais existentes:

NetworkManager
: O NetworkManager é desenvolvido especialmente para rede móvel em laptops. Oferece meios para troca fácil e automática de ambientes de rede ou tipos de rede diferentes como banda larga móvel (por exemplo, GPRS, EDGE ou 3G), LAN wireless e Ethernet. O NetworkManager suporta criptografia WEP e WPA-PSK em LANs wireless. Ele também suporta conexões discadas (com smpppd). Ambos os ambientes de área de trabalho (GNOME e KDE) incluem um front end para o NetworkManager. Para obter mais informações sobre os applets de área de trabalho, consulte a Seção 26.4, “Usando o KNetworkManager” (p 384) e a Seção 26.5, “Usando o applet NetworkManager do GNOME” (p 389).

Tabela 19.1 *Casos de uso para o NetworkManager*

Meu computador…	**Usar NetworkManager**
é um laptop	Sim
algumas vezes está conectado a redes diferentes	Sim
fornece serviços de rede (como DNS ou DHCP)	Não
usa somente um endereço IP estático	Não

Use as ferramentas do YaST para configurar a rede sempre que o NetworkManager não deve gerenciar a configuração de rede.

DICA: configuração DNS e vários tipos de conexões de rede

Se você viaja bastante com seu laptop e sempre muda para tipos de conexões de rede diferentes, o NetworkManager funcionará muito bem quando todos os endereços DNS forem atribuídos corretamente com DHCP. Se algumas das suas conexões usarem endereço(s) DNS estático(s), adicione-as à opção `NETCONFIG_DNS_STATIC_SERVERS` em `/etc/sysconfig/network/config`.

SLP

O SLP (Service Location Protocol) simplifica a conexão de um laptop a uma rede existente. Sem o SLP, o administrador do laptop normalmente necessita ter conhecimentos detalhados sobre os serviços disponíveis em uma rede. O SLP transmite a disponibilidade de um determinado tipo de serviço a todos os clientes de uma rede local. Os aplicativos que dão suporte ao SLP podem processar as informações despachadas pelo SLP e podem ser configurados automaticamente. O SLP também pode ser usado para instalar um sistema, minimizando o esforço de procurar uma fonte de instalação adequada. Encontre informações detalhadas sobre o SLP no Capítulo 24, *Serviços SLP na rede* (p 367).

19.1.3 Opções de software

Várias áreas de tarefas especiais no uso móvel ficam a cargo de software dedicado: monitoração do sistema (especialmente a carga da bateria), sincronização de dados e comunicação wireless com periféricos e com a Internet. As seguintes seções apresentam os aplicativos mais importantes que o SUSE Linux Enterprise Desktop oferece para cada tarefa.

19.1.3.1 Monitoração do sistema

Há duas ferramentas de monitoramento de sistema do KDE incluídas no SUSE Linux Enterprise Desktop:

Gerenciamento de Energia

Gerenciamento de Energia é um aplicativo que permite ajustar o comportamento relacionado à economia de energia da área de trabalho do KDE. Geralmente, é possível acessá-lo pelo ícone *Monitor de Bateria* na bandeja do sistema, que muda conforme o tipo de fonte de alimentação em uso. Outra maneira de abrir sua caixa de diálogo de configuração é através do *Lançador de Aplicativos Kickoff*: *Aplicativos* > *Configurar a Área de Trabalho* > *Avançado* > *Gerenciamento de Energia*.

Clique no ícone *Monitor de Bateria* na bandeja do sistema para acessar as opções para configurar seu comportamento. Você pode escolher um dos cinco perfis de energia exibidos que melhor atenda a suas necessidades. Por exemplo, o esquema *Apresentação* desabilita a proteção de tela e o gerenciamento de energia em geral, de modo que a sua apresentação não seja interrompida pelos eventos do sistema. Clique em *Mais...* para abrir uma tela de configurações mais complexas. Aqui você pode editar perfis individuais e definir opções avançadas de gerenciamento de energia e notificações, como o que fazer quando a tampa do laptop for fechada ou quando a bateria estiver baixa.

Monitor do Sistema

Monitor do Sistema (também chamado de *KSysguard*) coleta parâmetros de sistema mensuráveis em um ambiente de monitoramento. Apresenta as informações de saída em 2 guias por padrão. A *Tabela de Processos* fornece informações detalhadas sobre os processos em execução no momento, como carga de CPU, uso da memória ou número de ID e valor nice do processo. A apresentação e a filtragem dos dados coletados podem ser personalizadas: para adicionar um novo tipo de informação de processo, clique no cabeçalho da tabela de processos e escolha qual coluna

ocultar ou adicionar à tela. É possível também monitorar diferentes parâmetros do sistema em diversas páginas de dados ou coletar os dados de diversas máquinas em paralelo na rede. O KSysguard também pode ser executado como um daemon em máquinas desprovidas de um ambiente KDE. Encontre mais informações sobre esse programa na sua função de ajuda integrada ou nas páginas de ajuda do SUSE.

No ambiente do GNOME, use as *Preferências de Energia* e o *Monitor do Sistema*.

19.1.3.2 Sincronizando dados

Ao alternar entre o trabalho em uma máquina móvel desconectada da rede e o trabalho em uma estação em rede em um escritório, é necessário manter a sincronização dos dados processados em todas as instâncias. Isso pode incluir pastas de e-mail, diretórios e arquivos individuais que precisam estar presentes tanto para o trabalho remoto como para o trabalho no escritório. A solução nos dois casos é a seguinte:

Sincronizando e-mail
: Use uma conta IMAP para armazenar seus e-mails na rede empresarial. Em seguida, acesse os e-mails da estação de trabalho usando qualquer cliente de e-mail desconectado habilitado para IMAP, como Mozilla Thunderbird Mail, Evolution ou KMail, conforme descrito em *Guia do Usuário do GNOME* (↑*Guia do Usuário do GNOME*) e *KDE User Guide* (↑*KDE User Guide*). O cliente de e-mail precisa ser configurado de tal modo que as `Mensagens enviadas` sejam sempre acessadas da mesma pasta. Isso assegura a disponibilidade de todas as mensagens com informações sobre seu status após a conclusão do processo de sincronização. Use um servidor SMTP implementado no cliente de e-mail para enviar mensagens, em vez do sendmail ou postfix do MTA de todo o sistema para receber um feedback confiável sobre e-mails não enviados.

Sincronizando arquivos e diretórios
: Existem diversos utilitários adequados para a sincronização de dados entre um laptop e uma estação de trabalho. Um dos mais usados é uma ferramenta de área de trabalho chamada `rsync`. Para obter mais informações, consulte a respectiva página de manual (`man 1 rsync`)

19.1.3.3 Comunicação sem fio

Além da conexão a redes domésticas ou empresariais por cabo, também é possível fazer uma conexão wireless de um laptop para acessar outros computadores, periféricos,

telefones celulares ou PDAs. O Linux oferece suporte a três tipos de comunicação wireless:

WLAN
: Com o maior alcance dessas tecnologias wireless, a WLAN é a única adequada para a operação de redes de grande porte e, às vezes, até mesmo de redes virtualmente separadas. Máquinas individuais podem se conectar entre si para formar uma rede wireless independente ou para acessar a Internet. Dispositivos chamados de *pontos de acesso* atuam como estações de base para dispositivos habilitados para WLAN, além de servir como intermediários para o acesso à Internet. Um usuário móvel pode alternar entre pontos de acesso dependendo do local e de que ponto de acesso ofereça a melhor conexão. Assim como na telefonia celular, uma rede de grande porte está disponível aos usuários da WLAN sem restringi-los a um local específico para o acesso. Encontre informações sobre a WLAN no Capítulo 20, *Rede local sem fio* (p 257).

Bluetooth
: Entre todas as tecnologias wireless, o Bluetooth é a que possui o mais amplo espectro de aplicação. Ele pode ser usado na comunicação entre computadores (laptops) e PDAs ou telefones celulares, assim como o IrDA. Também pode ser utilizado para conectar diversos computadores dentro de uma extensão. O bluetooth também é usado para conectar componentes wireless do sistema, como um teclado ou mouse. Entretanto, o alcance dessa tecnologia não é suficiente para conectar sistemas remotos a uma rede. A WLAN é a melhor opção de tecnologia para comunicações em locais com obstáculos físicos, como paredes.

IrDA
: O IrDA é a tecnologia wireless de menor alcance. As duas extremidades da comunicação precisam estar a uma distância visível uma da outra. Não é possível contornar obstáculos como paredes. Uma aplicação possível do IrDA é a transmissão de arquivos de um laptop para um telefone celular. O curto caminho do laptop para o telefone celular é coberto com o uso do IrDA. O transporte de longo alcance do arquivo ao seu destinatário é feito pela rede móvel. Outra aplicação do IrDA é a transmissão wireless de serviços de impressão no escritório.

19.1.4 Segurança de dados

Em termos ideais, os dados contidos no seu laptop são protegidos de diversas maneiras contra o acesso não autorizado. Possíveis medidas de segurança podem ser tomadas nas seguintes áreas:

Proteção contra roubo
: Sempre que possível proteja a integridade física do seu sistema contra roubo. Diversas ferramentas de segurança (como correntes) podem ser adquiridas em lojas varejistas.

Autenticação avançada
: Use a autenticação biométrica juntamente com a autenticação padrão por meio de login e senha. O SUSE Linux Enterprise Desktop suporta autenticação por impressão digital. Para obter mais detalhes, consulte o Chapter 7, *Using the Fingerprint Reader* (↑*Security Guide*).

Protegendo dados no sistema
: Dados importantes devem ser criptografados não apenas durante a transmissão, mas também no disco rígido. Essa medida assegura sua segurança em caso de roubo. A criação de uma partição criptografada com o SUSE Linux Enterprise Desktop está descrita no Chapter 11, *Encrypting Partitions and Files* (↑*Security Guide*). Outra possibilidade é criar diretórios pessoais criptografados ao adicionar o usuário com o YaST.

IMPORTANTE: segurança de dados e o evento Suspender para Disco

As partições criptografadas não são desmontadas durante um evento de suspender para disco. Assim, todos os dados contidos nessas partições ficarão disponíveis para qualquer pessoa que conseguir roubar o hardware e inicializar o disco rígido.

Segurança da rede
: Qualquer transferência de dados deve ser segura, não importando como a transferência é feita. Para obter mais informações sobre problemas gerais de segurança referentes ao Linux e redes, consulte o Chapter 1, *Security and Confidentiality* (↑*Security Guide*). Medidas de segurança referentes a redes wireless são fornecidas no Capítulo 20, *Rede local sem fio* (p 257).

19.2 Hardware móvel

O SUSE Linux Enterprise Desktop suporta detecção automática de dispositivos de armazenamento móveis por FireWire (IEEE 1394) ou USB. O termo *dispositivo de armazenamento móvel* se aplica a qualquer tipo de disco rígido FireWire ou USB, unidade flash USB ou câmera digital. Esses dispositivos são automaticamente detectados e configurados logo após serem conectados ao sistema pela interface correspondente. Os gerenciadores de arquivos do GNOME e do KDE oferecem controle flexível de itens de hardware móveis. Para desmontar qualquer uma dessas mídias com segurança, use o recurso *Remover de Modo Seguro* (KDE) ou *Desmontar Volume* (GNOME) dos gerenciadores de arquivos. O gerenciamento de mídia removível pela área de trabalho é descrito em mais detalhes no *Guia do Usuário do GNOME* (↑*Guia do Usuário do GNOME*) e no *KDE User Guide* (↑*KDE User Guide*).

Discos rígidos externos (USB e FireWire)
: Assim que o disco rígido externo for corretamente reconhecido pelo sistema, seu ícone aparecerá no gerenciador de arquivos. Clique no ícone para exibir o conteúdo da unidade. É possível criar pastas e arquivos aqui, além de editá-los ou apagá-los. Para mudar o nome que um disco rígido recebeu do sistema, clique o botão direito do mouse no ícone e selecione o item correspondente no menu. Essa mudança de nome é limitada à exibição no gerenciador de arquivos. O descritor através do qual o dispositivo é montado em `/media` permanece não afetado por isso.

Unidades flash USB
: Esses dispositivos são tratados pelo sistema como discos rígidos externos. Também nesses dispositivos é possível renomear as entradas do gerenciador de arquivos.

Câmeras digitais (USB e FireWire)
: As câmeras digitais reconhecidas pelo sistema também aparecem como unidades externas na visão geral do gerenciador de arquivos. O KDE permite a leitura e o acesso às imagens no URL `camera:/`. Essas imagens podem ser processadas com o digiKam ou o f-spot. Para o processamento avançado de fotos, use o GIMP. Para obter uma introdução resumida do digiKam, do f-spot e do GIMP, consulte o Capítulo 18, *DigiKam: gerenciando sua coleção de imagens digitais* (↑*Guia de Aplicativos*), o Capítulo 19, *F-Spot: gerenciando sua coleção de imagens digitais* (↑*Guia de Aplicativos*) e o Capítulo 17, *GIMP: manipulando gráficos* (↑*Guia de Aplicativos*).

19.3 Telefones celulares e PDAs

Tanto um sistema de desktop como um laptop podem se comunicar com um telefone celular via Bluetooth ou IrDA. Alguns modelos dão suporte aos dois protocolos; outros, somente a um dos dois. As áreas de uso dos dois protocolos e a extensa documentação correspondente já foram citadas na Seção 19.1.3.3, "Comunicação sem fio" (p 251). A configuração desses protocolos nos telefones celulares é descrita nos respectivos manuais.

O suporte à sincronização com dispositivos portáteis fabricados pela Palm, Inc. já vem incorporado ao Evolution e ao Kontact. A conexão inicial com o dispositivo é facilmente realizada com um assistente. Após a configuração do suporte para Palm Pilots, é necessário determinar que tipo de dados deve ser sincronizado (endereços, compromissos etc.). Para obter mais informações, consulte *Guia do Usuário do GNOME* (↑*Guia do Usuário do GNOME*) e *KDE User Guide* (↑*KDE User Guide*).

Uma solução de sincronização mais sofisticada está disponível com o programa `opensync` (consulte o pacote libopensync e respectivos plug-ins de cada dispositivo).

19.4 Para obter mais informações

O ponto central de referência para todas as dúvidas relativas a dispositivos móveis e o Linux é http://tuxmobil.org/. Diversas seções desse site da Web tratam de aspectos de hardware e software de laptops, PDAs, telefones celulares e outros hardwares móveis.

Uma abordagem semelhante de http://tuxmobil.org/ é feita por http://www.linux-on-laptops.com/. Informações sobre laptops e dispositivos portáteis podem ser encontradas nesse local.

O SUSE mantém uma lista de discussão em alemão dedicada a laptops. Consulte http://lists.opensuse.org/opensuse-mobile-de/. Nesta lista, usuários e desenvolvedores discutem todos os aspectos da computação móvel com SUSE Linux Enterprise Desktop. As mensagens em inglês são respondidas, mas a maioria das informações dos arquivos está disponível somente em alemão. Use http://lists.opensuse.org/opensuse-mobile/ para ver postagens em inglês.

As informações sobre o OpenSync estão disponíveis em http://opensync.org/.

Rede local sem fio 20

As WLANs (Wireless Local Area Networks — redes locais wireless) passaram a ser um item indispensável na computação móvel. Atualmente, a maioria dos laptops tem placas WLAN embutidas. Este capítulo descreve como configurar uma placa WLAN com o YaST, criptografar transmissões e usar dicas. Se preferir, você poderá configurar e gerenciar o acesso a WLAN com o NetworkManager. Para obter informações detalhadas, consulte o Capítulo 26, *Usando o NetworkManager* (p 379).

20.1 Padrões de WLAN

As placas de WLAN comunicam-se usando o padrão 802.11, preparado pela organização IEEE. Originalmente, esse padrão fornecia uma taxa de transmissão máxima de 2 MBit/s. Enquanto isso, vários suplementos foram adicionados para aumentar a taxa de dados. Esses suplementos definem detalhes como modulação, saída de transmissão e taxas de transmissão (consulte a Tabela 20.1, “Visão geral de vários padrões de WLAN” (p 258)). Além disso, muitas empresas implementam hardware com recursos proprietários ou preliminares.

Tabela 20.1 Visão geral de vários padrões de WLAN

Nome	Banda (GHz)	Taxa de transmissão máxima (MBit/s)	Nota
802.11 Legado	2.4	2	Desatualizado; praticamente nenhum dispositivo final disponível
802.11a	5	54	Menos sujeito a interferência
802.11b	2.4	11	Menos comum
802.11g	2.4	54	Disseminado, compatível retroativamente com 11b
802.11n	2.4 e/ou 5	300	Comum
802.11 ad	2.4/5/60	até 7000	Lançado em 2012, menos comum atualmente

As placas 802.11 legadas não são suportadas pelo SUSE® Linux Enterprise Desktop. A maioria das placas que usa 802.11a, 802.11b, 802.11g e 802.11n é suportada. As placas novas geralmente são compatíveis com o padrão 802.11n, mas as placas que usam 802.11g ainda estão disponíveis.

20.2 Modos de funcionamento

Nas redes sem fio, várias técnicas e configurações são usadas para assegurar conexões rápidas, seguras e com alta qualidade. Tipos operacionais diferentes adaptam-se a configurações diferentes. Pode ser difícil escolher o método de autenticação correto. Os métodos de criptografia disponíveis possuem diferentes vantagens e armadilhas.

Basicamente, as redes wireless podem ser classificadas em três modos de rede:

Modo Gerenciado (Modo Infraestrutura), via Ponto de Acesso
: As redes gerenciadas têm um elemento de gerenciamento: o ponto de acesso. Nesse modo (também conhecido como modo de infraestrutura), todas as conexões das estações WLAN na rede passam pelo ponto de acesso, que também pode servir como uma conexão para uma ethernet. Para verificar se apenas as estações autorizadas poderão se conectar, vários mecanismos de autenticação (WPA, etc) são usados.

Modo Ad-hoc (Rede Ponto a Ponto)
: Redes ad-hoc não possuem um ponto de acesso. As estações se comunicam diretamente entre si, portanto, uma rede ad-hoc geralmente é mais rápida do que uma rede gerenciada. Entretanto, a faixa de transmissão e o número de estações participantes são muito limitados nas redes ad-hoc. Elas também não suportam autenticação WPA. Se você pretende usar a segurança WPA, não utilize o Modo Ad-Hoc.

Modo Mestre
: No modo master, a sua placa de rede é usada como ponto de acesso. Esse modo só funciona se a sua placa WLAN tiver suporte. Os detalhes sobre a sua placa WLAN encontram-se em `http://linux-wless.passys.nl`.

20.3 Autenticação

Como uma rede sem fio é muito mais fácil de interceptar e comprometer do que uma rede com fio, os vários padrões incluem métodos de autenticação e criptografia. Na versão original do padrão IEEE 802.11, esses métodos são descritos sob o termo WEP (Wired Equivalent Privacy — privacidade equivalente à das redes com fio). Porém, como o WEP se demonstrou inseguro (consulte a Seção 20.6.3, “Segurança” (p 271)), o setor de WLAN (unificado sob o nome *Wi-Fi Alliance*) definiu uma extensão

denominada WPA, que supostamente elimina os pontos fracos do WEP. O último padrão IEEE 802.11i inclui WPA e alguns outros métodos de autenticação e criptografia. O IEEE 802.11i também é chamado de WPA2, pois o WPA é baseado em uma versão de rascunho do 802.11i.

Para garantir que apenas as estações autorizadas possam se conectar, vários mecanismos de autenticação são usados em redes gerenciadas:

Nenhum (aberto)
: Um sistema aberto é um sistema que não precisa de autenticação. Qualquer estação pode se juntar à rede. Entretanto, a criptografia WEP pode ser usada, consulte a Seção 20.4, "Criptografia" (p 261).

Chave compartilhada (de acordo com o padrão IEEE 802.11)
: Nesse procedimento, a chave WEP é usada para autenticação. Porém, esse procedimento não é recomendado, porque torna a chave WEP mais suscetível a ataques. Tudo o que um invasor precisa fazer é escutar durante tempo suficiente a comunicação entre a estação e o ponto de acesso. Durante o processo de autenticação, ambos os lados trocam as mesmas informações, uma vez de forma criptografada e outra de forma não criptografada. Isso possibilita a reconstrução da chave com as ferramentas adequadas. Como esse método utiliza a chave WEP para a autenticação e para a criptografia, ele não melhora a segurança da rede. Uma estação com a chave WEP correta pode ser autenticada, criptografada e descriptografada. Uma estação que não tem a chave não pode descriptografar os pacotes recebidos. Da mesma maneira, ela não pode se comunicar, mesmo que tenha que se autenticar.

WPA-PSK (ou WPA-Personal, de acordo com o IEEE 802.1x)
: O WPA-PSK (PSK corresponde a preshared key — chave pré-compartilhada) funciona de maneira semelhante ao procedimento Chave compartilhada. Todas as estações participantes, assim como o ponto de acesso, precisam da mesma chave. A chave tem 256 bits de tamanho e normalmente é digitada como uma frase secreta. Esse sistema não precisa de um gerenciamento de chave complexo como o WPA-EAP e é mais adequado para uso privado. Portanto, o WPA-PSK é às vezes conhecido como WPA "Home".

WPA-EAP (ou WPA-Enterprise, de acordo com o IEEE 802.1x)
: Na verdade, o WPA-EAP (Extensible Authentication Protocol) não é um sistema de autenticação, e sim um protocolo para transporte de informações de autenticação. O WPA-EAP é usado para proteger redes sem fio em empresas. Em redes privadas,

ele é raramente usado. Por esse motivo, o WPA-EAP é às vezes conhecido como WPA “Enterprise”.

O WPA-EAP precisa de um servidor Radius para autenticar os usuários. O EAP oferece três métodos diferentes de conexão e autenticação no servidor:

- TLS (Transport Layer Security) (EAP-TLS): A autenticação TLS utiliza o intercâmbio mútuo de certificados para o servidor e o cliente. Primeiro, o servidor apresenta o seu certificado para o cliente, onde ele é avaliado. Se o certificado for considerado válido, o cliente, por sua vez, apresenta o seu certificado para o servidor. Embora o TLS seja seguro, ele exige uma infraestrutura de gerenciamento de certificação que funcione em sua rede. Essa infraestrutura é raramente encontrada em redes particulares.

- Tunneled Transport Layer Security (EAP-TTSL)

- Protected Extensible Authentication Protocol (EAP-PEAP): Ambos TTLS e PEAP são protocolos de dois estágios. No primeiro estágio, uma conexão segura é estabelecida e, no segundo, os dados de autenticação do cliente são trocados. Eles exigem muito menos overhead de gerenciamento de certificação do que o TLS, se houver.

20.4 Criptografia

Existem vários métodos de criptografia para assegurar que pessoas não autorizadas não possam ler os pacotes de dados que são trocados em uma rede sem fio nem obter acesso à rede:

WEP (definido no padrão IEEE 802.11)

Esse padrão utiliza o algoritmo de criptografia RC4, originalmente com um tamanho de chave de 40 bits, posteriormente também com 104 bits. Muitas vezes, o tamanho é declarado como 64 bits ou 128 bits, dependendo da inclusão ou não dos 24 bits do vetor de inicialização. Porém, esse padrão tem algumas fraquezas. Os ataques contra as chaves geradas por esse sistema podem ser bem-sucedidos. Contudo, é melhor usar o WEP do que não criptografar a rede de maneira alguma.

Alguns fornecedores implementaram o “WEP Dinâmico” não padrão. Ele funciona exatamente como o WEP e compartilha os mesmos pontos fracos, exceto pelo fato

de que a chave é mudada periodicamente por um serviço de gerenciamento de chave.

TKIP (definido no padrão WPA/IEEE 802.11i)
: Esse protocolo de gerenciamento de chave definido no padrão WPA utiliza o mesmo algoritmo de criptografia do WEP, mas elimina sua fraqueza. Como uma nova chave é gerada para cada pacote de dados, os ataques contra essas chaves são infrutíferos. O TKIP é usado junto com o WPA-PSK.

CCMP (definido no padrão IEEE 802.11i)
: O CCMP descreve o gerenciamento de chave. Normalmente, ele é usado na conexão com o WPA-EAP, mas também pode ser usado com o WPA-PSK. A criptografia acontece de acordo com o AES e é mais forte do que a criptografia RC4 do padrão WEP.

20.5 Configuração com o YaST

IMPORTANTE: Riscos à segurança em redes wireless

As conexões de WLAN não criptografadas permitem que terceiros interceptem todos os dados da rede. Proteja o tráfego de sua rede usando um dos métodos de autenticação e criptografia suportados.

Use o melhor método de criptografia possível que o seu hardware permitir. No entanto, para usar determinado método de criptografia, todos os dispositivos na rede devem suportar esse método; do contrário, eles não poderão se comunicar. Por exemplo, se o seu roteador suporta tanto WEP quanto WPA, mas o driver da sua placa WLAN só suporta WEP, WEP será o mínimo denominador comum que você poderá usar. Mesmo assim, uma criptografia fraca com WEP é melhor que nada. Consulte a Seção 20.4, “Criptografia” (p 261) e a Seção 20.6.3, “Segurança” (p 271) para obter mais informações.

Para configurar uma LAN wireless com o YaST, defina os seguintes parâmetros:

Endereço IP
: Use o endereço IP estático ou permita que um servidor DHCP atribua dinamicamente um endereço IP à interface.

Modo de funcionamento
: Define como integrar sua máquina à WLAN, de acordo com a topologia de rede. Para obter mais informações de apoio sobre o , consulte a Seção 20.2, “Modos de funcionamento” (p 259).

Nome da Rede (ESSID)
: String exclusiva que identifica a rede.

Detalhes da Autenticação e da Criptografia
: Dependendo do método de autenticação e criptografia usado pela sua rede, você precisará inserir uma ou mais chaves e/ou certificados.

  Várias opções de entrada estão disponíveis para inserir as respectivas chaves: *Passphrase*, *ASCII* (disponível apenas para os métodos de autenticação WEP) e *Hexadecimal*.

20.5.1 Desativando o NetworkManager

Uma placa WLAN geralmente é detectada durante a instalação. Se a sua máquina for um computador móvel, o NetworkManager normalmente será ativado por padrão. Para configurar a placa WLAN com o YaST, você precisa primeiro desativar o NetworkManager:

1. Inicie o YaST como usuário `root`.

2. No Centro de Controle do YaST, selecione *Dispositivos de Rede* > *Configurações de Rede* para abrir a caixa de diálogo *Configurações de Rede*.

   Se a sua rede for controlada pelo NetworkManager, você verá uma mensagem de aviso explicando que as configurações de rede não podem ser editadas pelo YaST.

3. Para habilitar a edição com o YaST, saia da mensagem clicando em *OK* e, na guia *Opções Globais*, ative *Método Tradicional com ifup*.

4. Para saber mais sobre a configuração, vá para a Seção 20.5.2, “Configuração para pontos de acesso” (p 264) ou a Seção 20.5.3, “Estabelecendo uma rede ad-hoc” (p 268).

   Do contrário, confirme as suas mudanças clicando em *OK* para gravar a configuração de rede.

20.5.2 Configuração para pontos de acesso

Nesta seção, saiba como configurar a placa WLAN para conexão (externa) com um ponto de acesso ou como usar a placa WLAN como um ponto de acesso, se a sua placa WLAN suportar esse recurso. Para ver a configuração de redes sem um ponto de acesso, consulte a Seção 20.5.3, "Estabelecendo uma rede ad-hoc" (p 268).

Procedimento 20.1 *Configurando a placa WLAN para usar um ponto de acesso*

1. Inicie o YaST e abra a caixa de diálogo *Configurações de Rede*.

2. Passe para a guia *Visão Geral*, na qual são listadas todas as placas de rede que foram detectadas pelo sistema. Se você precisar de mais informações sobre a configuração geral da rede, consulte a Seção 23.4, "Configurando uma conexão de rede com o YaST" (p 318).

3. Escolha sua placa wireless na lista e clique em *Editar* para abrir a caixa de diálogo Configuração da Placa de Rede.

4. Na guia *Endereço*, configure se será usado um endereço IP dinâmico ou estático para a máquina. Normalmente, *Endereço Dinâmico* com *DHCP* é o ideal.

5. Clique em *Avançar* para prosseguir para a caixa de diálogo *Configuração de Placa de Rede Wireless*.

6. Para usar a placa WLAN para conexão com um ponto de acesso, defina o *Modo de Operação* como *Gerenciado*.

   Mas para usar a placa WLAN como ponto de acesso, defina o *Modo de Operação* como *Mestre*. Observe que nem todas as placas WLAN suportam esse modo.

   NOTA: Usando WPA-PSK ou WPA-EAP

   Para usar os modos de autenticação WPA-PSK ou WPA-EAP, o modo de operação deve ser definido como *Gerenciado*.

   ---

7. Para conectar-se a determinada rede, digite o *Nome de Rede (ESSID)*. Se preferir, clique em *Verificar Rede* e selecione uma rede na lista de redes wireless disponíveis.

   Todas as estações em uma rede sem fio precisam do mesmo ESSID para se comunicar umas com as outras. Se nenhum ESSID for especificado, sua placa WLAN será

associada automaticamente ao ponto de acesso que tiver a melhor intensidade de sinal.

NOTA: A autenticação WPA requer um ESSID

Se você selecionar a autenticação *WPA*, será preciso definir um nome de rede (ESSID).

---

8 Selecione um *Modo de Autenticação* para a rede. O modo adequado depende do driver da placa WLAN e da capacidade dos outros dispositivos na rede.

9 Se você definiu o *Modo de Autenticação* como *Sem Criptografia*, termine a configuração clicando em *Avançar*. Confirme a mensagem sobre esse possível risco à segurança e saia da guia *Visão Geral* (que mostra a placa WLAN recém-configurada) clicando em *OK*.

Se escolheu qualquer um dos outros modos de autenticação, proceda com Procedimento 20.2, "Inserindo os detalhes da criptografia" (p 266).

Figura 20.1 *YaST: configurando a placa de rede wireless*

Procedimento 20.2 *Inserindo os detalhes da criptografia*

Os métodos de autenticação a seguir requerem uma chave criptográfica: *WEP - Aberto*, *WEP - Chave Compartilhada* e *WPA-PSK*.

Para WEP, em geral, apenas uma chave é necessária; porém, até 4 chaves WEP diferentes podem ser definidas na estação. Uma delas deve ser definida como a chave padrão e deve ser usada para a criptografia. As outras são usadas para a decodificação. Por padrão, o tamanho da chave de 128 bits é usado, mas também é possível definir o tamanho como 64 bits.

Para maior segurança, o WPA-EAP usa o servidor RADIUS para autenticar os usuários. Para autenticação no servidor, três métodos diferentes estão disponíveis: TLS, TTLS e PEAP. As credenciais e os certificados necessários para o WPA-EAP dependem do método de autenticação usado no servidor RADIUS. Peça ao administrador do sistema para fornecer as informações e credenciais necessárias. O YaST procura por certificados em `/etc/cert`. Portanto, grave os certificados concedidos a você nesse local e restrinja o acesso a esses arquivos para `0600` (leitura e gravação pelo proprietário).

1 Para digitar a chave para *WEP - Aberto* ou *WEP - Chave Compartilhada*:

1a Defina o *Tipo de Chave de Entrada* como *Passphrase*, *ASCII* ou *Hexadecimal*.

1b Digite a respectiva *Chave de Criptografia* (geralmente, uma única chave é usada):

Se você selecionou *Passphrase*, digite uma palavra ou uma string de caracteres da qual a chave será gerada de acordo com o tamanho de chave especificado (por padrão, 128 bits) .

O ASCII exige uma entrada de 5 caracteres para uma chave de 64 bits e 13 caracteres para uma chave de 128 bits.

Para a opção *Hexadecimal*, digite 10 caracteres para uma chave de 64 bits ou 26 caracteres para uma chave de 128 bits em notação hexadecimal.

1c Para ajustar o tamanho da chave a uma taxa de bits menor (o que pode ser necessário para hardware mais antigo), clique em *Chaves WEP* e defina o *Tamanho de Chave* como *64* bits. A caixa de diálogo *Chaves WEP* também mostra as chaves WEP que foram inseridas até o momento. A menos que

outra chave seja explicitamente definida como padrão, o YaST sempre usará a primeira chave como padrão.

1d Para digitar mais chaves para o WEP ou modificar uma das chaves, selecione a respectiva entrada e clique em *Editar*. Selecione o *Tipo de Chave de Entrada* e digite a chave.

1e Confirme as mudanças clicando em *OK*.

2 Para digitar a chave para *WPA-PSK*:

2a Selecione o método de entrada *Passphrase* ou *Hexadecimal*.

2b Digite a respectiva *Chave de Criptografia*.

No modo *Frase Secreta*, a entrada deve ser de 8 a 63 caracteres. No modo *Hexadecimal*, digite 64 caracteres.

3 Se você escolheu a autenticação *WPA-EAP*, clique em *Avançar* para alternar para a caixa de diálogo *WPA-EAP*, na qual você insere as credenciais e os certificados recebidos pelo administrador de rede.

3a Selecione o *Modo EAP* que o servidor RADIUS usa para autenticação. Os detalhes necessários para inserir os dados a seguir dependem do *Modo EAP* selecionado.

3b Para TLS, especifique *Identidade*, *Certificado de Cliente*, *Chave do Cliente* e *Senha da Chave do Cliente*. Para aumentar a segurança, é possível configurar um *Certificado de Servidor* usado para validar a autenticidade do servidor.

TTLS e PEAP requerem *Identidade* e *Senha*, enquanto *Certificado de Servidor* e *Identidade Anônima* são opcionais.

3c Para acessar a caixa de diálogo de autenticação avançada para a configuração do WPA-EAP, clique em *Detalhes*.

3d Selecione o *Método de Autenticação* para o segundo estágio da comunicação EAP-TTLS ou EAP-PEAP (autenticação interna). A escolha dos métodos depende do método de autenticação para o servidor RADIUS selecionado na caixa de diálogo anterior.

3e Se a configuração determinada automaticamente não funcionar para você, escolha uma *Versão PEAP* específica para forçar o uso de determinada implementação PEAP.

4 Confirme as mudanças clicando em *OK*. A guia *Visão Geral* mostra os detalhes da sua placa WLAN recém-configurada.

5 Clique em *OK* para finalizar a configuração e sair da caixa de diálogo.

20.5.3 Estabelecendo uma rede ad-hoc

Em alguns casos, é útil conectar dois computadores equipados com uma placa WLAN. Para estabelecer uma rede ad hoc usando o YaST, faça o seguinte:

1 Inicie o YaST e abra a caixa de diálogo *Configurações de Rede*.

2 Mude para a guia *Visão Geral*, escolha sua placa wireless na lista e clique em *Editar* para abrir a caixa de diálogo *Configuração da Placa de Rede*.

3 Escolha *Endereço IP Atribuído Estaticamente*OBJ e digite os seguintes dados:

- *Endereço IP*: `192.168.1.1`. Mude esse endereço no segundo computador para `192.168.1.2`, por exemplo.
- *Máscara da Sub-rede*: `/24`
- *Nome de Host*: escolha qualquer nome que desejar.

4 Continue com *Avançar*.

5 Defina o *Modo de Operação* como *Ad-hoc*.

6 Escolha um *Nome da Rede (ESSID)*. Pode ser qualquer nome, mas deve ser usado em todos os computadores na rede ad-hoc.

7 Selecione um *Modo de Autenticação* para a rede. O modo adequado depende do driver da placa WLAN e da capacidade dos outros dispositivos na rede.

8. Se você definiu o *Modo de Autenticação* como *Sem Criptografia*, termine a configuração clicando em *Avançar*. Confirme a mensagem sobre esse possível risco à segurança e saia da guia *Visão Geral*, que mostra a placa WLAN recém-configurada, clicando em *OK*.

   Se escolheu qualquer um dos outros modos de autenticação, proceda com o Procedimento 20.2, "Inserindo os detalhes da criptografia" (p 266).

9. Caso não tenha o `smpppd` instalado, o YaST pedirá para você fazer isso.

10. Configure outras placas WLAN na rede de acordo, usando o mesmo *Nome de Rede (ESSID)*, o mesmo *Modo de Autenticação*, mas endereços IP diferentes.

20.5.4 Definindo parâmetros de configuração adicionais

Normalmente, não é necessário mudar as configurações predefinidas durante a configuração da placa WLAN. Porém, se você precisa de uma configuração detalhada da sua conexão WLAN, o YaST permite ajustar as seguintes configurações:

Canal
: A especificação de um canal em que a estação WLAN deve trabalhar. Isso é necessário apenas nos modos *Ad-hoc* e *Mestre*. No modo *Gerenciado*, a placa pesquisa automaticamente os canais disponíveis para pontos de acesso.

Taxa de Bits
: Dependendo do desempenho da sua rede, você pode definir uma determinada taxa de bits para a transmissão de um ponto para outro. Na configuração padrão *Automático*, o sistema tenta usar a taxa de transmissão de dados mais alta possível. Algumas placas WLAN não suportam a configuração da taxa de bits.

Access Point (Ponto de Acesso)
: Em um ambiente com vários pontos de acesso, um deles pode ser pré-selecionado especificando-se o endereço MAC.

Gerenciamento de energia
: Quando você estiver em trânsito, as tecnologias de economia de energia poderão ajudá-lo a maximizar o tempo de operação da sua bateria. Mais informações sobre o gerenciamento de energia estão disponíveis no Capítulo 21, *Gerenciamento de*

energia (p 275). O uso do gerenciamento de energia pode afetar a qualidade da conexão e aumentar a latência da rede.

Para acessar as opções avançadas:

1. Inicie o YaST e abra a caixa de diálogo *Configurações de Rede*.
2. Mude para a guia *Visão Geral*, escolha sua placa wireless na lista e clique em *Editar* para abrir a caixa de diálogo *Configuração da Placa de Rede*.
3. Clique em *Avançar* para prosseguir para a caixa de diálogo *Configuração de Placa de Rede Wireless*.
4. Clique em *Configurações de Especialista*.
5. No modo *Ad-hoc*, selecione um dos canais oferecidos (11 a 14, dependendo do seu país) para a comunicação da sua estação com as outras estações. No modo *Mestre*, determine em que *Canal* a placa deve oferecer a funcionalidade de ponto de acesso. A configuração padrão para esta opção é *Auto*.
6. Selecione a *Taxa de Bits* a ser usada.
7. Digite o endereço MAC do *Ponto de Acesso* ao qual deseja se conectar.
8. Escolha se vai *Usar Gerenciamento de Energia* ou não.
9. Confirme as suas mudanças clicando em *OK* e clique em *Avançar* e em *OK* para concluir a configuração.

20.6 Dicas sobre a configuração de uma WLAN

As seguintes ferramentas e dicas o ajudam a monitorar e melhorar a velocidade, a estabilidade e os aspectos de segurança da WLAN.

20.6.1 Utilitários

O pacote wireless-tools contém utilitários que permitem definir parâmetros específicos para WLAN e obter estatísticas. Consulte http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html para obter mais informações.

20.6.2 Estabilidade e velocidade

O desempenho e a confiabilidade de uma rede wireless dependem principalmente do fato de as estações participantes receberem um sinal sem criptografia das outras estações. Obstruções como paredes podem enfraquecer grandemente o sinal. Quanto menor a força do sinal, mais lenta fica a transmissão. Durante a operação, verifique a intensidade do sinal com o utilitário iwconfig na linha de comando (campo Qualidade do Link) ou com os applets do NetworkManager fornecidos pelo KDE ou GNOME. Se tiver problemas com a qualidade do sinal, tente configurar os dispositivos em outro lugar ou ajuste a posição das antenas do seu ponto de acesso. Antenas auxiliares que melhoram substancialmente a recepção estão disponíveis para várias placas PCMCIA WLAN. A taxa especificada pelo fabricante, como 54 MBit/s, é um valor nominal que representa o máximo teórico. Na prática, o throughput máximo de dados não passa da metade desse valor.

O comando iwspy exibe as estatísticas da WLAN:

```
iwspy wlan0
wlan0      Statistics collected:
    00:AA:BB:CC:DD:EE : Quality:0  Signal level:0  Noise level:0
    Link/Cell/AP      : Quality:60/94  Signal level:-50 dBm   Noise level:-140
 dBm (updated)
    Typical/Reference : Quality:26/94  Signal level:-60 dBm   Noise level:-90
 dBm
```

20.6.3 Segurança

Se você desejar configurar uma rede sem fio, lembre-se de que qualquer pessoa dentro da faixa de transmissão poderá acessá-la facilmente se não forem implementadas medidas de segurança. Portanto, certifique-se de ativar o método de criptografia. Todas as placas WLAN e pontos de acesso suportam a criptografia WEP. Embora não seja completamente segura, ela representa um obstáculo para um invasor em potencial.

Para uso particular, use WPA-PSK, se disponível. Embora o Linux suporte WPA na maioria dos componentes de hardware, alguns drivers não oferecem suporte a WPA. É possível também que ele não esteja disponível em pontos de acesso e roteadores mais antigos com a funcionalidade WLAN. Para esses dispositivos, verifique se o WPA pode ser implementado por meio de uma atualização de firmware. Se o WPA não estiver disponível, é melhor utilizar a criptografia WEP do que nenhum tipo de criptografia. Em empresas com requisitos de segurança avançados, as redes sem fio devem ser operadas somente com WPA.

Use senhas avançadas para o seu método de autenticação. Por exemplo, a página na Web `https://www.grc.com/passwords.htm` gera senhas aleatórias de 64 caracteres.

20.7 Solução de problemas

Se a sua placa WLAN não responder, verifique os seguintes pré-requisitos:

1. Você sabe o nome do dispositivo da placa WLAN? Geralmente é `wlan0`. Verifique com a ferramenta `ifconfig`.

2. Você verificou o firmware necessário? Consulte `/usr/share/doc/packages/wireless-tools/README.firmware` para obter mais informações.

3. O ESSID do seu roteador é transmitido e está visível (não está oculto)?

20.7.1 Verificar o status da rede

O comando `iwconfig` pode fornecer informações importantes sobre a sua conexão wireless. Por exemplo, a linha a seguir exibe o ESSID, o modo wireless, a frequência, se o sinal está criptografado, a qualidade do link e muito mais:

```
iwconfig wlan0
wlan0  IEEE 802.11abg  ESSID:"guest"
       Mode:Managed   Frequency:5.22GHz  Access Point: 00:11:22:33:44:55
       Bit Rate:54 Mb/s   Tx-Power=13 dBm
       Retry min limit:7   RTS thr:off   Fragment thr:off
       Encryption key:off
       Power Management:off
       Link Quality:62/92   Signal level:-48 dBm  Noise level:-127 dBm
```

```
       Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
       Tx excessive retries:10  Invalid misc:0   Missed beacon:0
```

Você também pode obter as informações anteriores com o comando `iwlist`. Por exemplo, a linha a seguir exibe a taxa de bits atual:

```
iwlist wlan0 rate
wlan0    unknown bit-rate information.
         Current Bit Rate=54 Mb/s
```

Se desejar uma visão geral de quantos pontos de acesso estão disponíveis, use o comando `iwlist`. Ele mostra uma lista das “células” com a seguinte aparência:

```
iwlist wlan0 scanning
wlan0   Scan completed:
   Cell 01 - Address: 00:11:22:33:44:55
             Channel:40
             Frequency:5.2 GHz (Channel 40)
             Quality=67/70  Signal level=-43 dBm
             Encryption key: off
             ESSID:"Guest"
             Bit Rates: 6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s;
                        24 Mb/s; 36 Mb/s; 48 Mb/s
             Mode: Master
             Extra:tsf=0000111122223333
             Extra: Last beacon: 179ms ago
             IE: Unknown: ...
```

20.7.2 Vários dispositivos de rede

Laptops modernos geralmente têm uma placa de rede e uma placa WLAN. Se você configurar ambos os dispositivos com DHCP (atribuição de endereço automática), poderá encontrar problemas com a resolução de nome e o gateway padrão. Isso fica evidente quando você pode efetuar ping no roteador, mas não pode navegar na Internet. O Banco de Dados de Suporte no endereço http://old-en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clients apresenta um artigo sobre o assunto.

20.7.3 Problemas com placas Prism2

Vários drivers estão disponíveis para dispositivos com chips Prism2. As várias placas funcionam mais ou menos adequadamente com os vários drivers. Com essas placas, a criptografia WPA somente pode ser usada com o driver hostap. Se tal placa não funcionar

adequadamente ou não funcionar ou se você desejar usar a criptografia WPA, leia /usr/share/doc/packages/wireless-tools/README.prism2.

20.8 Para obter mais informações

Mais informações encontram-se nas seguintes páginas:

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html
: As páginas da Internet de Jean Tourrilhes, que desenvolveu as *Ferramentas Sem Fio* para o Linux, apresentam uma grande variedade de informações sobre dispositivos sem fio.

http://tuxmobil.org
: Informações práticas úteis sobre computadores móveis com Linux.

http://www.linux-on-laptops.com
: Mais informações sobre Linux em laptops.

Gerenciamento de energia 21

O gerenciamento de energia é especialmente importante em laptops, mas também é útil em outros sistemas. A ACPI (Advanced Configuration and Power Interface — Interface de Energia e Configuração Avançada) está disponível em todos os computadores modernos (laptops, desktops e servidores). As tecnologias de gerenciamento de energia exigem hardware adequado e rotinas BIOS. A maioria dos laptops e muitos desktops e servidores modernos atendem a esses requisitos. Também é possível controlar a escala de frequência de CPU para economizar energia ou reduzir o ruído.

21.1 Funções de economia de energia

As funções de economia de energia não são significativas apenas para o uso móvel de laptops, como também para sistemas desktop. As funções principais e respectivas utilizações na ACPI são:

Standby
: Não suportado.

Suspender (para memória)
: Este modo grava todo o estado do sistema na memória RAM. Em seguida, todo o sistema é colocado em repouso, salvo a memória RAM. Neste estado, o computador consome pouquíssima energia. A vantagem desse estado é a possibilidade de reiniciar o trabalho no mesmo ponto em alguns segundos sem precisar inicializar e reiniciar os aplicativos. Essa função corresponde ao estado da ACPI `S3`.

Suspender (para o disco)
: Neste modo operacional, o estado do sistema inteiro é gravado no disco rígido e o sistema é desligado. Deve existir uma partição de troca pelo menos tão grande quanto a RAM para gravar todos os dados ativos. A reativação desse estado leva de 30 a 90 segundos. O estado anterior ao suspenso é restaurado. Alguns fabricantes oferecem variantes híbridas desse modo, como RediSafe em Thinkpads da IBM. O estado correspondente da ACPI é `S4`. No Linux, a suspensão para disco é desempenhada pelas rotinas de kernel, que são independentes de ACPI.

Monitor de bateria
: A ACPI verifica o status da carga da bateria e fornece informações correspondentes. Além disso, ela coordena as ações a serem desempenhadas quando um status de carga crítico é atingido.

Desligamento automático
: Após um encerramento, o computador é desligado. Isto é especialmente importante quando um encerramento automático é realizado pouco antes da bateria esgotar-se.

Controle de velocidade do processador
: Em conexão com a CPU, é possível economizar energia de três maneiras diferentes: escala de frequência e voltagem (também conhecida como PowerNow! ou Speedstep), throttling e adormecimento do processador (C-states). Dependendo do modo operacional do computador, esses métodos também podem ser combinados.

21.2 Advanced Configuration and Power Interface (ACPI)

A ACPI foi desenvolvida para habilitar o sistema operacional a configurar e controlar cada componente de hardware. A ACPI substitui tanto o Plug and Play (PnP) de Gerenciamento de Energia quanto o Gerenciamento Avançado de Energia (APM). Ela envia informações sobre a bateria, o adaptador de CA, a temperatura, o ventilador e eventos do sistema, como “fechar tampa” ou “bateria fraca”.

O BIOS fornece tabelas que contém informações sobre os componentes individuais e métodos de acesso ao hardware. O sistema operacional usa essas informações para tarefas como atribuir interrupções ou ativar e desativar componentes. Como o sistema operacional executa comandos armazenados no BIOS, a funcionalidade depende da

implementação do BIOS. As tabelas que a ACPI podem detectar e carregar são reportadas em `/var/log/boot.msg`. Consulte a Seção 21.2.2, "Solução de problemas" (p 277) para obter mais informações sobre solução de problemas da ACPI.

21.2.1 Controlando o desempenho da CPU

A CPU pode economizar energia de três maneiras:

- Escala de frequência e voltagem
- Obstruindo a frequência do relógio (T-states)
- Adormecendo o processador (C-states)

Dependendo do modo operacional do computador, estes métodos também podem ser combinados. Economizar energia também significa que o sistema esquenta menos e os ventiladores são ativados com menos frequência.

Expansão e throttling de frequência são relevantes apenas quando o processador está ocupado, pois o C-state mais econômico é aplicado de qualquer maneira quando o processador fica ocioso. Se a CPU estiver ocupada, a escala da frequência é o método recomendado para economia de energia. Em geral o processador só trabalha com carga parcial. Neste caso, pode ser executado com uma frequência inferior. Normalmente, a expansão da frequência dinâmica controlada pelo regulador sob demanda do kernel é a melhor abordagem.

Throttling deve ser usado como última alternativa, por exemplo, para ampliar o tempo de operação da bateria, apesar de uma alta carga do sistema. Contudo, alguns sistemas não são executados suavemente quando ocorrem throttlings em excesso. Ademais, o throttling da CPU não faz sentido se a CPU tem pouco a fazer.

Para obter informações mais detalhadas, consulte o Chapter 11, *Power Management* (↑*System Analysis and Tuning Guide*).

21.2.2 Solução de problemas

Há dois tipos de problemas. De um lado, o código ACPI do kernel pode conter erros que não foram detectados em tempo útil. Neste caso, uma solução estará disponível para download. O mais comum é que os problemas sejam causados pelo BIOS. Às

vezes, desvios da especificação da ACPI são propositalmente integrados ao BIOS para contornar erros na implementação da ACPI em outros sistemas operacionais amplamente utilizados. Componentes de hardware que têm erros sérios na implementação da ACPI são gravados em uma lista negra que impede que o kernel do Linux use a ACPI para esses componentes.

A primeira ação a ser tomada quando problemas forem detectados, é atualizar o BIOS. Se o computador não inicializar de jeito nenhum, um dos seguintes parâmetros de boot poderá ser útil:

pci=noacpi
: Não usar ACPI para configurar os dispositivos PCI.

acpi=ht
: Realizar apenas uma configuração com recursos simples. Não usar a ACPI para outros fins.

acpi=off
: Desabilitar a ACPI.

ATENÇÃO: problemas de boot sem ACPI

Algumas máquinas mais novas (especialmente os sistemas SMP e AMD64) precisam de ACPI para configurar o hardware corretamente. Nestas máquinas, desabilitar a ACPI pode causar problemas.

Às vezes a máquina é confundida pelo hardware conectado por USB ou FireWire. Se uma máquina se recusa a inicializar, desconecte todos os itens de hardware desnecessários e tente novamente.

Monitore as mensagens de boot do sistema com o comando `dmesg | grep -2i acpi` (ou todas as mensagens, porque o problema pode não ser causado pela ACPI) após o boot. Se ocorrer um erro ao analisar uma tabela ACPI, a tabela mais importante, a DSDT (*Differentiated System Description Table*), poderá ser substituída por uma versão aprimorada. Neste caso, a DSDT defeituosa do BIOS é ignorada. O procedimento está descrito na Seção 21.4, “Solução de problemas” (p 281).

Na configuração do kernel, há um switch para ativar as mensagens de depuração da ACPI. Se houver um kernel com depuração ACPI compilado e instalado, serão emitidas informações detalhadas.

Se você tiver problemas com BIOS ou hardware, é sempre recomendável entrar em contato com os fabricantes. Especialmente se eles nem sempre derem assistência ao Linux, devem ser indagados em caso de problemas. Os fabricantes só levarão a questão a sério se compreenderem que um número satisfatório de seus clientes usa Linux.

21.2.2.1 Para obter mais informações

- `http://tldp.org/HOWTO/ACPI-HOWTO/` (ACPI HOWTO detalhado, contém patches DSDT)
- `http://www.acpi.info` (Configuração Avançada e Especificação da Interface de Energia)
- `http://www.lesswatts.org/projects/acpi/` (O projeto ACPI4Linux em Sourceforge)
- `http://acpi.sourceforge.net/dsdt/index.php` (Patches DSDT por Bruno Ducrot)

21.3 Descanso do disco rígido

No Linux, o disco rígido pode colocado em repouso total se não estiver em uso e pode ser executado em modo mais econômico ou silencioso. Nos laptops modernos, não é necessário desativar o disco rígido manualmente, porque entram automaticamente em um modo operacional econômico sempre que não estão em uso. No entanto, para aumentar a economia de energia, experimente alguns dos seguintes métodos usando o comando `hdparm`.

Ele pode ser usado para modificar várias configurações de disco rígido. A opção `-y` alterna instantaneamente o disco rígido para o modo standby. `-Y` coloca-o em repouso. `hdparm -S x` faz o disco rígido ser encerrado após um determinado período de inatividade. Substitua *x* conforme a seguir: `0` desabilita esse mecanismo, fazendo o disco rígido funcionar continuamente. Valores de `1` a `240` são multiplicados por 5 segundos. Valores de `241` a `251` correspondem de 1 a 11 vezes 30 minutos.

As opções de economia de energia interna do disco rígido podem ser controladas pela opção `-B`. Selecione um valor de `0` a `255` para obter de economia máxima a throughput

máximo. O resultado depende do disco rígido usado e é difícil de avaliar. Para tornar um disco rígido mais silencioso, use a opção `-M`. Selecione um valor de `128` a `254` para obter de silencioso a rápido.

Muitas vezes não é fácil colocar o disco rígido em repouso. No Linux, vários processos gravam no disco rígido, ativando-o repetidamente. Portanto, é importante entender como o Linux trata os dados que necessitam ser gravados no disco rígido. Primeiro, todos os dados estão no buffer da memória RAM. Esse buffer é monitorado pelo daemon `pdflush`. Quando os dados atingem uma determinada idade limite ou quando o buffer está cheio até certo grau, o conteúdo do buffer é descarregado para o disco rígido. O tamanho do buffer é dinâmico e depende do tamanho da memória e da carga do sistema. Por padrão, pdflush é configurado em intervalos curtos para obter a integridade máxima de dados. Ele verifica o buffer a cada 5 segundos e grava os dados no disco rígido. As seguintes variáveis são interessantes:

`/proc/sys/vm/dirty_writeback_centisecs`
: Inclui o atraso até o thread pdflush ser acionado (em centésimos de segundo).

`/proc/sys/vm/dirty_expire_centisecs`
: Define o período após o qual uma página modificada deve ser gravada por último. O padrão é `3000`, o que equivale a 30 segundos.

`/proc/sys/vm/dirty_background_ratio`
: Porcentagem máxima de páginas modificadas para pdflush começar a gravá-las. O padrão é `5`%.

`/proc/sys/vm/dirty_ratio`
: Quando a página modificada exceder essa porcentagem da memória total, os processos são forçados a gravar buffers modificados durante suas frações de tempo em vez de continuar gravando.

ATENÇÃO: deficiência da integridade de dados

Qualquer modificação nas configurações do daemon `pdflush` coloca em risco a integridade dos dados.

Além desses processos, sistemas JFS, como `Btrfs`, `Ext3`, `Ext4` entre outros, gravam seus metadados independentemente do `pdflush`, que também impede que o disco rígido pare de funcionar. Para evitar isso, foi desenvolvida uma extensão especial de

kernel para dispositivos móveis. Para usar a extensão, instale o pacote `laptop-mode-tools` e consulte `/usr/src/linux/Documentation/laptops/laptop-mode.txt` para ver os detalhes.

Outro fator importante é o modo como se comportam os programas ativos. Por exemplo, os bons editores gravam regularmente backups ocultos do arquivo modificado no momento para o disco rígido, fazendo com que ele saia do modo de hibernação. Recursos como este podem ser desabilitados às custas da integridade dos dados.

Com relação a isso, o mail daemon postfix faz uso da variável `POSTFIX_LAPTOP`. Se essa variável for configurada para `sim`, postfix acessa o disco rígido com muito menos frequência.

No SUSE Linux Enterprise Desktop, estas tecnologias são controladas por `laptop-mode-tools`.

21.4 Solução de problemas

Todas as mensagens de erro e alertas são registradas no arquivo `/var/log/messages`. As seções a seguir abordam os problemas mais comuns.

21.4.1 ACPI ativada com suporte de hardware, mas funções não funcionam

Se tiver problemas com a ACPI, procure nos resultados de `dmesg` por mensagens específicas da ACPI, utilizando o comando `dmesg|grep -i acpi`.

Poderá ser necessário atualizar o BIOS para solucionar o problema. Na home page do fabricante do seu laptop, procure uma versão atualizada do BIOS e instale-a. Peça ao fabricante para estar em conformidade com a última especificação da ACPI. Se os erros persistirem após a atualização do BIOS, faça o seguinte para substituir a tabela DSDT defeituosa no seu BIOS com um DSDT atualizado:

Procedimento 21.1 *Atualizando a tabela DSDT no BIOS*

Para o procedimento a seguir, verifique se estes pacotes estão instalados: `kernel-source`, `pmtools` e `mkinitrd`.

1. Faça o download do DSDT para o seu sistema em `http://acpi.sourceforge.net/dsdt/index.php`. Verifique se o arquivo está descompactado e compilado como mostra a extensão de arquivo `.aml` (linguagem computacional ACPI). Se for o caso, continue com a etapa 3.

2. Se a extensão de arquivo da tabela descarregada for `.asl` (linguagem de origem da ACPI), compile-a executando o seguinte comando:

   ```
   iasl -sa file.asl
   ```

3. Copie o arquivo (resultante) `DSDT.aml` para qualquer local (`/etc/DSDT.aml` é recomendado).

4. Edite `/etc/sysconfig/kernel` e adapte o caminho para o arquivo DSDT de forma compatível.

5. Inicie o `mkinitrd`. Sempre que você instalar o kernel e usar o `mkinitrd` para criar um arquivo `initrd`, a DSDT modificada será integrada e carregada quando o sistema for inicializado.

21.4.2 A frequência da CPU não funciona

Consulte as fontes do kernel para ver se o seu processador é suportado. Você poderá precisar de um módulo de kernel ou de opção especial para ativar o controle de frequência da CPU. Se o pacote `kernel-source` estiver instalado, essas informações estarão disponíveis em `/usr/src/linux/Documentation/cpu-freq/*`.

21.4.3 Suspender e Standby não funcionam

Os sistemas ACPI podem ter problemas com suspender e standby devido a falha na implementação de DSDT (BIOS). Se esse for o seu caso, atualize o BIOS.

Quando o sistema tenta descarregar módulos defeituosos, o sistema é verificado ou o evento suspenso não é acionado. O mesmo também pode acontecer se você não descarregar módulos ou interromper serviços que impeçam uma suspensão bem-sucedida. Em ambos os casos, tente identificar o módulo defeituoso que impediu o modo adormecido. O arquivo de registro `/var/log/pm-suspend.log` contém informações detalhadas sobre o que está ocorrendo e onde estão os erros possíveis. Modifique a variável `SUSPEND_MODULES` em `/usr/lib/pm-utils/defaults` para descarregar os módulos com problema antes de efetuar suspensão ou standby.

21.5 Para obter mais informações

- `http://en.opensuse.org/SDB:Suspend_to_RAM`: Como fazer o recurso Suspender para RAM funcionar

- `http://old-en.opensuse.org/Pm-utils`: Como modificar a metodologia geral de suspensão

22 Usando Tablet PCs

O SUSE® Linux Enterprise Desktop oferece suporte a Tablet PCs. A seguir, você aprenderá a instalar e configurar seu Tablet PC e descobrirá alguns aplicativos do Linux* úteis que aceitam entrada de canetas digitais.

Os seguintes Tablet PCs são suportados:

- Tablet PCs com dispositivos multitoque, de tela sensível ao toque ou tablet (baseado em caneta) Wacom de série e USB.
- Tablet PCs com dispositivos FinePoint, como Gateway C210X/M280E/CX2724 ou HP Compaq TC1000.
- Tablet PCs com dispositivos de tela sensível ao toque, como Asus R2H, Clevo TN120R, Fujitsu Siemens Computers série P, LG C1 e Samsung Q1/Q1-Ultra.

Depois que você instalar os pacotes do Tablet PC e configurar seu digitalizador corretamente, a entrada com a caneta (também chamada de stylus) poderá ser usada para as seguintes ações e aplicativos:

- Efetuar login no KDM ou GDM
- Desbloquear sua tela nas áreas de trabalho KDE e GNOME
- Ações que também pode ser acionadas por outros dispositivos apontadores (como mouse ou touch pad), por exemplo, mover o cursor na tela, iniciar aplicativos, fechar, redimensionar e mover janelas, deslocar o foco da janela, e arrastar e soltar objetos
- Usar o reconhecimento de gestos nos aplicativos do sistema X Window

- Desenhar com o GIMP
- Fazer anotações ou criar esboços com aplicativos como o Jarnal ou o Xournal ou editar quantidades maiores de texto com o Dasher

22.1 Instalando pacotes do Tablet PC

Os pacotes necessários para Tablet PCs estão incluídos no padrão de instalação `TabletPC`; se ele foi selecionado durante a instalação, os seguintes pacotes já deverão estar instalados no sistema:

- `cellwriter`: um painel de entrada de escrita à mão com base em caracteres
- `jarnal`: um aplicativo baseado em Java para anotações
- `xournal`: um aplicativo para anotações e esboços
- `xstroke`: um programa de reconhecimento de gestos para o Sistema X Window
- `xvkbd`: um teclado virtual para o Sistema X Window
- `x11-input-fujitsu`: o módulo de entrada X para tablets Fujitsu série P
- `x11-input-evtouch`: o módulo de entrada X para alguns Tablet PCs com telas sensíveis ao toque
- `xorg-x11-driver-input`: o módulo de entrada X para dispositivos de entrada, incluindo o módulo para dispositivos Wacom.

Se esses pacotes não estiverem instalados, instale manualmente os pacotes necessários da linha de comando ou selecione o padrão `TabletPC` para instalação no YaST.

22.2 Configurando seu dispositivo tablet

Durante a instalação, o tablet ou dispositivo de toque é configurado por padrão. Caso tenha problemas com a configuração do dispositivo Wacom, use `xsetwacom` na linha de comando para mudar as configurações.

22.3 Usando o teclado virtual

Para efetuar login na área de trabalho do KDE ou do GNOME ou desbloquear a tela, você pode digitar seu nome de usuário e senha da maneira normal ou por meio do teclado virtual (xvkbd), exibido abaixo do campo de login. Para configurar o teclado ou acessar a ajuda integrada, clique no campo *xvkbd* no canto inferior esquerdo para abrir o menu principal do xvkbd.

Se sua entrada não estiver visível (ou não for transferida para a janela onde necessário), redirecione o foco clicando na tecla *Foco* no xvkbd e clicando na janela que deve receber os eventos do teclado.

Figura 22.1 *Teclado virtual xvkbd*

Se você quiser usar o xvkbd após o login, inicie-o por meio do menu principal ou com `xvkbd` de um shell.

22.4 Girando a tela

Use o KRandRTray (KDE) ou o gnome-display-properties (GNOME) para girar ou redimensionar sua tela de forma manual e simultânea. Tanto o KRandRTray quanto o gnome-display-properties são applets para a extensão RANDR do servidor X.

Inicie o KRandRTray ou o gnome-display-properties do menu principal ou digite `krandrtray` ou `gnome-display-properties` para iniciar o applet de um shell. Após iniciar o applet, seu ícone geralmente é adicionado à sua bandeja do sistema. Se o ícone do gnome-display-properties não aparecer automaticamente na bandeja do sistema, verifique se *Mostrar Telas no Painel* está ativado na caixa de diálogo *Configurações de Resolução do Monitor*.

Para girar sua tela com o KRandRTray, clique o botão direito do mouse no ícone e selecione *Configurar Tela*. Selecione a orientação desejada na caixa de diálogo de configuração.

Para girar a tela com gnome-display-properties, clique o botão direito do mouse no ícone e selecione a orientação desejada. A tela é inclinada imediatamente na nova direção. A orientação do tablet de gráficos também muda, para que ainda possa interpretar o movimento da caneta corretamente.

Se tiver problemas ao mudar a orientação da sua área de trabalho, consulte a Seção 22.7, “Solução de problemas” (p 293) para obter mais informações.

Para obter mais informações sobre os applets específicos da área de trabalho da extensão RANDR, consulte a Section “Monitor Settings” (Chapter 3, *Customizing Your Settings*, ↑*KDE User Guide*) e a Seção “Configurando telas” (Capítulo 3, *Personalizando suas configurações*, ↑*Guia do Usuário do GNOME*).

22.5 Usando o reconhecimento de gestos

O SUSE Linux Enterprise Desktop inclui o CellWriter e o xstroke para reconhecimento de gestos. Ambos os aplicativos aceitam gestos executados com a caneta ou outros dispositivos apontadores como entrada para os aplicativos no Sistema X Window.

22.5.1 Usando o CellWriter

Com o CellWriter, você pode escrever caracteres em uma grade de células. A escrita é reconhecida instantaneamente a cada caractere. Após terminar de escrever, você pode enviar a entrada para o aplicativo em foco no momento. Antes de se poder usar o CellWriter para reconhecimento de gestos, o aplicativo precisa ser treinado para reconhecer sua caligrafia: você precisa treinar cada caractere de um determinado mapa de teclas (caracteres não treinados não são ativados e, portanto, não podem ser usados).

Procedimento 22.1 *Treinando o CellWriter*

1. Inicie o CellWriter no menu principal ou com `cellwriter` na linha de comando. Na primeira inicialização, o CellWriter entra automaticamente em modo de treino. No modo de treino, mostra um conjunto de caracteres do mapa de teclas escolhido no momento.

2. Insira o gesto que gostaria de usar para um caractere em sua respectiva célula. Com a primeira entrada, o fundo tem sua cor modificada para branco, embora o caractere apareça em cinza claro. Repita o gesto várias vezes até a cor do caractere mudar para preto. Caracteres não instruídos são mostrados em um fundo cinza claro ou marrom (dependendo do esquema de cores da área de trabalho).

3. Repita essa etapa até ter treinado o CellWriter para todos os caracteres de que você precisa.

4. Se desejar treinar o CellWriter para outro idioma, clique no botão *Configuração* e selecione um idioma da guia *Idiomas*. *Feche* a caixa de diálogo de configuração. Clique no botão *Treinar* e selecione o mapa de teclas na caixa suspensa no canto inferior direito da janela do *CellWriter*. Agora repita seu treino para o novo mapa de teclas.

5. Após terminar o treino para o mapa de teclas, clique no botão *Treinar* para alternar para o modo normal.

No modo normal, a janela do CellWriter mostra algumas células vazias nas quais inserir os gestos. Os caracteres não são enviados a outro aplicativo até você clicar no botão *Inserir*, para que possa corrigir ou apagar caracteres antes de usá-los como entrada. Os caracteres que tiverem sido reconhecidos com baixo grau de confiança aparecerão realçados. Para corrigir sua entrada, use o menu de contexto que aparece ao se clicar com o botão direito do mouse em uma célula. Para apagar um caractere, use a borracha

da sua caneta ou clique no meio com o mouse para limpar a célula. Após terminar sua entrada no CellWriter, defina qual aplicativo deve recebê-la clicando na janela desse aplicativo. Em seguida, envie a entrada para o aplicativo clicando em *Inserir*.

Figura 22.2 *Reconhecimento de gestos com o CellWriter*

Ao clicar no botão *Teclas* do CellWriter, você obtém um teclado virtual que pode ser usado em vez do reconhecimento de caligrafia.

Para ocultar o CellWriter, feche sua janela. O aplicativo agora aparece como um ícone na bandeja do sistema. Para mostrar a janela de entrada novamente, clique no ícone da bandeja do sistema.

22.5.2 Usando o Xstroke

Com o xstroke, você pode usar gestos com sua caneta ou outros dispositivos apontadores como entrada para aplicativos no Sistema X Window. O alfabeto do xstroke é um alfabeto de traço único semelhante ao alfabeto Graffiti*. Quando ativado, o xstroke envia a entrada à janela atualmente focalizada.

1. Inicie o KRandRTray por meio do menu principal ou com `xstroke` em um shell. Isso adiciona um ícone de lápis à bandeja do sistema.

2. Inicie o aplicativo para o qual deseja criar a entrada de texto com a caneta (por exemplo, uma janela de terminal, um editor de texto ou o LibreOffice Writer).

3. Para ativar o modo de reconhecimento de gestos, clique no ícone de lápis uma vez.

4. Execute alguns gestos no tablet de gráficos com a caneta ou outro dispositivo apontador. O xstroke captura os gestos e transfere-os para o texto que é exibido na janela do aplicativo focalizado.

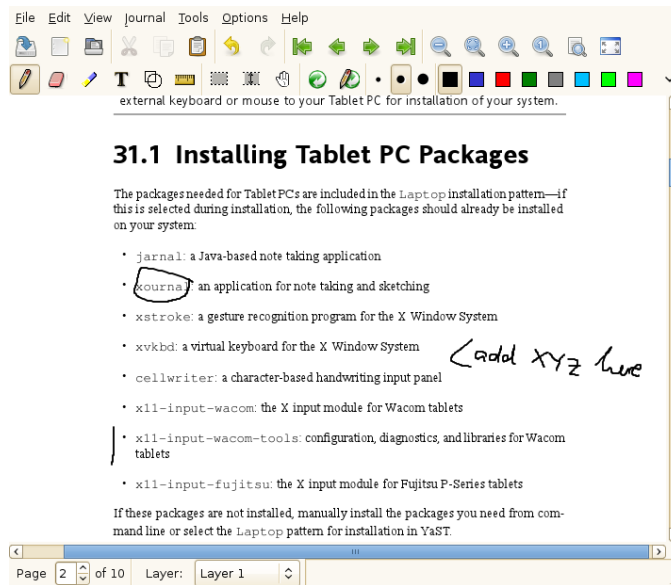
5 Para alternar o foco para uma janela diferente, clique na janela desejada com a caneta e mantenha o botão do mouse pressionado por um momento (ou use o atalho do teclado definido no centro de controle de sua área de trabalho).

6 Para desativar o modo de reconhecimento de gestos, clique no ícone de lápis novamente.

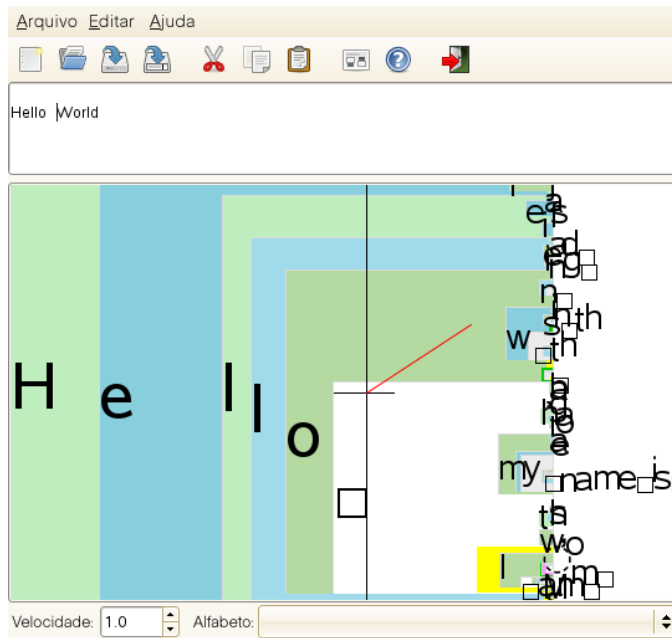
22.6 Fazendo anotações e criando esboços com a caneta

Para criar desenhos com a caneta, use um editor de gráficos profissional, como o GIMP, ou experimente um aplicativo de anotações, Xournal ou Jarnal. Com o Xournal e o Jarnal, você pode fazer anotações, criar desenhos ou inserir comentários em arquivos PDF com a caneta. Como um aplicativo baseado em Java disponível para diversas plataformas, o Jarnal também oferece recursos básicos de colaboração. Para obter mais informações, consulte `http://www.dklevine.com/general/software/tc1000/jarnal-net.htm`. Ao gravar seu conteúdo, o Jarnal armazena os dados em um formato de arquivo (*.jaj) que também contém um arquivo no formato SVG.

Inicie o Jarnal ou Xournal por meio do menu principal ou digitando `jarnal` ou `xournal` em um shell. Para inserir comentários en um arquivo PDF no Xournal, por exemplo, selecione *File (Arquivo)* > *Annotate PDF (Anotar PDF)* e abra o arquivo PDF em seu sistema de arquivos. Use a caneta ou outro dispositivo de ponteiro para anotar o PDF e grave as mudanças com *Arquivo* > *Exportar para PDF*.

Figura 22.3 Fazendo anotações em um PDF com o Xournal

O Dasher é outro aplicativo útil. Foi projetado para situações em que a entrada pelo teclado não é prática ou não está disponível. Com algum treinamento, você pode digitar rapidamente quantidades maiores de texto usando somente a caneta (ou outros dispositivos de entrada — é possível até usar um rastreador de visão).

Inicie o Dasher por meio do menu principal ou com`dasher` em um shell. Mova sua caneta em uma direção e o aplicativo começará a ampliar as letras no lado direito. Com as letras que passam pelo meio do cursor de linha cruzada, o texto é criado ou previsto e é impresso na parte superior da janela. Para começar ou parar de escrever, clique na tela uma vez com a caneta. Modifique a velocidade de zoom na parte inferior da janela.

Figura 22.4 Editando textos com o Dasher

O conceito do Dasher funciona para muitos idiomas. Para obter mais informações, consulte o site na Web do Dasher, que oferece documentação, demonstrações e textos de treinamento abrangentes. Encontre-o em `http://www.inference.phy.cam.ac.uk/dasher/`

22.7 Solução de problemas

O teclado virtual não aparece na tela de login

Ocasionalmente, o teclado virtual não é exibido na tela de login. Para resolver isso, reinicie o servidor X pressionando Ctrl + Alt + <— ou pressione a tecla apropriada em seu Tablet PC (se você usar um modelo plano sem teclado integrado). Se o teclado virtual ainda não for exibido, conecte um teclado externo a seu modelo plano e efetue logon usando o teclado do hardware.

A orientação dos tablets de gráficos com Wacom não muda

Com o comando `xrandr`, você pode mudar a orientação de sua tela por meio de um shell. Digite `xrandr --help` para ver as opções disponíveis. Para mudar

simultaneamente a orientação de seu tablet de gráficos, o comando precisa ser modificado conforme descrito abaixo:

- Para a orientação normal (rotação de 0°):

```
xrandr -o normal && xsetwacom --set "Serial Wacom Tablet" Rotate
NONE
```

- Para a rotação de 90° (no sentido horário, retrato):

```
xrandr -o right && xsetwacom --set "Serial Wacom Tablet" Rotate CW
```

- Para a rotação de 180° (paisagem):

```
xrandr -o inverted && xsetwacom --set "Serial Wacom Tablet" Rotate
HALF
```

- Para a rotação de 270° (no sentido anti-horário, retrato):

```
xrandr -o left && xsetwacom set --"Serial Wacom Tablet" Rotate CCW
```

Observe que os comandos acima dependem da saída do comando `xsetwacom list`. Substitua `"Serial Wacom Tablet"` pela saída do dispositivo de toque ou stylus. Se tiver um dispositivo Wacom com suporte a toque (você usa os dedos na tela para mover o cursor), será necessário girar o dispositivo de toque.

22.8 Para obter mais informações

Alguns dos aplicativos mencionados aqui não oferecem ajuda on-line integrada, mas você pode encontrar informações úteis sobre o uso e a configuração em seu sistema instalado em `/usr/share/doc/package/packagename` ou na Web:

- Para obter o manual do Xournal, consulte http://xournal.sourceforge.net/manual.html
- A documentação do Jarnal está localizada em http://jarnal.wikispaces.com/
- Obtenha a página de manual do xstroke em http://davesource.com/Projects/xstroke/xstroke.txt
- Obtenha um documento HOWTO para configurar X no site na Web do Wacom sobre Linux: http://sourceforge.net/apps/mediawiki/linuxwacom/index.php?title=Configuring_X
- Obtenha um site na Web bastante informativo sobre o projeto do Dasher em http://www.inference.phy.cam.ac.uk/dasher/
- Obtenha mais informações e documentação sobre o CellWriter em http://risujin.org/cellwriter/
- Informações sobre o gnome-display-properties podem ser obtidas em http://old-en.opensuse.org/GNOME/Multiscreen

Parte IV. Serviços

23 Rede básica

O Linux oferece os recursos e as ferramentas de rede necessários para a integração em todos os tipos de estruturas de rede. O acesso à rede por meio de placa de rede, modem ou outro dispositivo pode ser configurado com o YaST. A configuração também pode ser feita manualmente. Neste capítulo são abordados apenas os mecanismos fundamentais e os arquivos de configuração de rede relevantes.

Linux e outros sistemas operacionais Unix usam o protocolo TCP/IP. Não é um protocolo de rede único, mas uma família de protocolos de rede que oferece vários serviços. Os protocolos listados na Tabela 23.1, "Vários protocolos na família de protocolos TCP/IP" (p 300) são fornecidos com a finalidade de trocar dados entre duas máquinas por meio do TCP/IP. As redes combinadas por TCP/IP compõem uma rede mundial também chamada de "Internet".

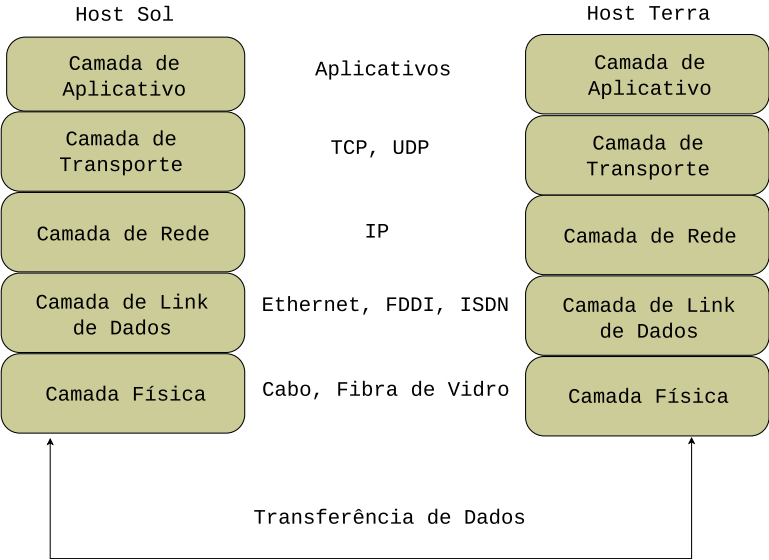
RFC significa *Request for Comments*. Os RFCs são documentos que descrevem vários procedimentos de implementação e protocolos da Internet para o sistema operacional e seus aplicativos. Os documentos RFC descrevem a configuração dos protocolos da Internet. Para ampliar seus conhecimentos sobre qualquer dos protocolos, consulte os documentos de RFC apropriados. Eles estão disponíveis em `http://www.ietf.org/rfc.html`.

Tabela 23.1 Vários protocolos na família de protocolos TCP/IP

Protocolo	Descrição
TCP	Transmission Control Protocol: um protocolo seguro orientado por conexão. Os dados a serem transmitidos são enviados primeiramente pelo aplicativo como fluxo de dados e convertidos no formato adequado ao sistema operacional. Os dados chegam ao respectivo aplicativo no host de destino com o formato original de fluxo de dados no qual foram inicialmente enviados. O TCP determina se algum dado foi perdido ou embaralhado durante a transmissão. O TCP é implementado onde a sequência de dados for necessária.
UDP	User Datagram Protocol: um protocolo inseguro, não baseado em conexão. Os dados a serem transmitidos são enviados na forma de pacotes gerados pelo aplicativo. A ordem em que os dados chegam ao destinatário não é garantida, havendo possibilidade de perda dos dados. O UDP é adequado para aplicativos orientados por registro. Ele possui um período de latência menor que o TCP.
ICMP	Internet Control Message Protocol: essencialmente, não se trata de um protocolo para o usuário final, mas um protocolo de controle especial que emite relatórios de erros e pode controlar o comportamento de

Protocolo	Descrição
	máquinas que participam da transferência de dados TCP/IP. Além disso, ele fornece um modo de eco especial, que pode ser visualizado usando o programa ping.
IGMP	Internet Group Management Protocol: esse protocolo controla o comportamento da máquina na implementação de multicast IP.

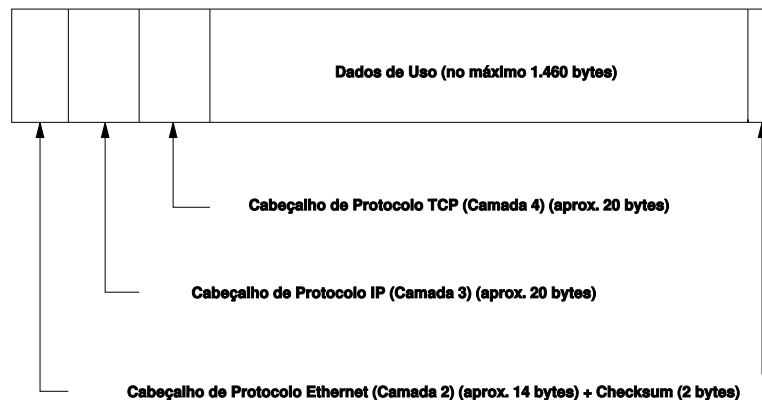
Conforme mostrado na Figura 23.1, "Modelo de camadas simplificado para TCP/IP" (p 301), a troca de dados ocorre em camadas diferentes. A camada de rede real é a transferência de dados insegura por IP (Internet protocol). Acima do IP, o TCP garante, até certo ponto, a segurança na transferência de dados. A camada IP é suportada pelo protocolo dependente de hardware subjacente, como uma ethernet.

Figura 23.1 *Modelo de camadas simplificado para TCP/IP*

O diagrama fornece um ou dois exemplos para cada camada. As camadas são organizadas de acordo com os *níveis de abstração*. A camada mais baixa fica muito próxima do hardware. A camada mais alta é quase completamente abstraída do hardware. Todas as camadas possuem suas funções especiais próprias. As funções especiais de cada camada, na maioria das vezes, estão implícitas em suas descrições. O link de dados e as camadas físicas representam a rede física usada, como uma ethernet.

Quase todos os protocolos de hardware funcionam em uma base orientada por pacotes. Os dados a serem transmitidos são reunidos em *pacotes* (não podem ser enviados todos de uma vez). O tamanho máximo de um pacote TCP/IP é de, aproximadamente, 64 KB. Os pacotes são normalmente bem menores, já que o hardware da rede pode ser um fator de limitação. O tamanho máximo de um pacote de dados em uma ethernet é em torno de 1.500 bytes. O tamanho de um pacote TCP/IP limita-se a esse máximo quando os dados são enviados por uma ethernet. Se mais dados forem transferidos, mais pacotes de dados precisarão ser enviados pelo sistema operacional.

Para que as camadas executem suas respectivas funções, informações adicionais referentes a cada uma delas devem ser gravadas no pacote de dados. Isso ocorre no *cabeçalho* do pacote. Todas as camadas anexam um pequeno bloco de dados, chamado cabeçalho do protocolo, à frente de cada pacote emergente. Um exemplo de um pacote de dados TCP/IP transmitido por um cabo ethernet é exibido na Figura 23.2, “Pacote Ethernet TCP/IP” (p 302). A soma de teste está localizada no final do pacote e não no início. Isso torna as coisas mais simples para o hardware de rede.

Figura 23.2 *Pacote Ethernet TCP/IP*

Dados de Uso (no máximo 1.460 bytes)
Cabeçalho de Protocolo TCP (Camada 4) (aprox. 20 bytes)
Cabeçalho de Protocolo IP (Camada 3) (aprox. 20 bytes)
Cabeçalho de Protocolo Ethernet (Camada 2) (aprox. 14 bytes) + Checksum (2 bytes)

Quando um aplicativo envia dados por uma rede, eles passam por cada camada, todas implementadas no kernel do Linux, exceto a camada física. Cada camada é responsável

pela preparação dos dados, para que eles possam passar para a camada seguinte. A camada mais baixa é a responsável pelo envio de dados. Todo o processo é invertido quando os dados são recebidos. Como camadas de uma cebola, em cada uma os cabeçalhos de protocolo são removidos dos dados transportados. Por fim, a camada de transporte é responsável por disponibilizar os dados para uso pelos aplicativos de destino. Dessa forma, cada camada se comunica somente com a camada diretamente acima ou abaixo dela. Para os aplicativos, é irrelevante o fato de os dados serem transmitidos por uma rede FDDI de 100 MBit/s ou por uma linha de modem de 56 kbit/s. Da mesma forma, é irrelevante para a linha de dados os tipos de dados transmitidos, contanto que os pacotes estejam no formato correto.

23.1 Roteamento e endereços IP

Esta seção limita-se à abordagem de redes IPv4. Para obter informações sobre o protocolo IPv6, sucessor do IPv4, consulte a Seção 23.2, “IPv6 — A Internet da próxima geração” (p 306).

23.1.1 Endereços IP

Todo computador na Internet possui um endereço de 32 bits exclusivo. Esses 32 bits (ou 4 bytes) são normalmente gravados conforme ilustrado na segunda linha no Exemplo 23.1, “Gravando endereços IP” (p 303).

Exemplo 23.1 *Gravando endereços IP*

```
IP Address (binary):  11000000 10101000 00000000 00010100
IP Address (decimal):      192.     168.       0.      20
```

Na forma decimal, os quatro bytes são gravados no sistema de números decimais, separados por pontos. O endereço IP é designado a um host ou a uma interface de rede. Ele pode ser usado apenas uma vez em todo o mundo. Há exceções a essa regra, mas não são relevantes para as passagens a seguir.

Os pontos nos endereços IP indicam o sistema hierárquico. Até os anos 90, os endereços IP eram estritamente categorizados em classes. Entretanto, esse sistema demonstrou ser excessivamente inflexível e foi desativado. Agora, o *CIDR* (Classless Interdomain Routing — Roteamento Interdomínio sem Classes) é usado.

23.1.2 Máscaras de rede e roteamento

As máscaras de rede são usadas para definir a faixa de endereços de uma sub-rede. Se dois hosts estiverem na mesma sub-rede, eles podem ter contato direto. Se não estiverem na mesma sub-rede, eles precisarão do endereço de um gateway que gerencie todo o tráfego da sub-rede. Para verificar se dois endereços IP estão em uma mesma sub-rede, basta "E" os dois endereços com a máscara de rede. Se o resultado for idêntico, os dois endereços IP estarão na mesma rede local. Se houver diferenças, o endereço IP remoto e, portanto, a interface remota, só poderão ser localizados através de um gateway.

Para compreender como as máscaras de rede funcionam, consulte o Exemplo 23.2, "Vinculando endereços IP à máscara de rede" (p 304). A máscara de rede consiste em 32 bits que identificam quanto de um endereço IP pertence à rede. Todos os bits `1` marcam o bit correspondente no endereço IP como pertencente à rede. Todos os bits `0` marcam os bits dentro da sub-rede. Isso significa que quanto maior a quantidade de bits `1`, menor será o tamanho da sub-rede. Como a máscara de rede sempre consiste em vários bits `1` sucessivos, também é possível apenas contar o número de bits da máscara de rede. No Exemplo 23.2, "Vinculando endereços IP à máscara de rede" (p 304) a primeira rede com 24 bits também poderia ser gravada como `192.168.0.0/24`.

Exemplo 23.2 *Vinculando endereços IP à máscara de rede*

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
---------------------------------------------------------------
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:           192.     168.       0.       0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask    (255.255.255.0): 11111111 11111111 11111111 00000000
---------------------------------------------------------------
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:           213.      95.      15.       0
```

Um outro exemplo: todas as máquinas conectadas ao mesmo cabo ethernet, normalmente, estão localizadas na mesma sub-rede e são diretamente acessíveis. Mesmo quando a sub-rede é dividida fisicamente por switches ou pontes, esses hosts ainda assim podem ser diretamente localizados.

Endereços IP fora da sub-rede local só poderão ser localizados se um gateway for configurado para a rede de destino. Nos casos mais comuns, há somente um gateway

que controla todo o tráfego externo. Entretanto, também é possível configurar vários gateways para sub-redes diferentes.

Se um gateway tiver sido configurado, todos os pacotes IP externos serão enviados para o gateway apropriado. Esse gateway tentará então encaminhar os pacotes da mesma forma (de host para host) até acessar o host de destino ou até o TTL (time to live) do pacote expirar.

Tabela 23.2 *Endereços específicos*

Tipo de endereço	Descrição
Endereço de rede base	Essa é a máscara de rede E qualquer endereço na rede, conforme mostrado no Exemplo 23.2, "Vinculando endereços IP à máscara de rede" (p 304) em `Resultado`. Esse endereço não pode ser designado a nenhum host.
Endereço de broadcast	Isso significa, basicamente, "Acessar todos os hosts nesta sub-rede." Para gerar isso, a máscara de rede é invertida no formato binário e vinculada ao endereço de rede base com um OU lógico. Portanto, o exemplo acima resulta em 192.168.0.255. Esse endereço não pode ser atribuído a nenhum host.
Host local	O endereço `127.0.0.1` é designado ao "dispositivo loopback" em cada host. Pode-se configurar uma conexão para a sua própria máquina com este endereço e com todos os endereços da rede de loopback completa `127.0.0.0/8`, conforme definidos com o IPv4. Com o IPv6, existe apenas um endereço de loopback (`::1`).

Como os endereços IP precisam ser exclusivos em qualquer parte do mundo, não é possível selecionar endereços aleatoriamente. Há três domínios de endereços a serem usados para configurar uma rede baseada em IP privado. Eles não conseguem se conectar ao restante da Internet, pois não podem ser transmitidos através dela. Esses domínios de endereço são especificados no RFC 1597 e listados na Tabela 23.3, "Domínios de endereços IP privados" (p 306).

Tabela 23.3 *Domínios de endereços IP privados*

Rede/máscara de rede	Domínio
`10.0.0.0/255.0.0.0`	`10.x.x.x`
`172.16.0.0/255.240.0.0`	`172.16.x.x – 172.31.x.x`
`192.168.0.0/255.255.0.0`	`192.168.x.x`

23.2 IPv6 — A Internet da próxima geração

Devido ao surgimento da WWW (World Wide Web), a Internet teve um crescimento acelerado com um número cada vez maior de computadores se comunicando por TCP/IP nos últimos quinze anos. Desde que Tim Berners-Lee da CERN (`http://public.web.cern.ch`) inventou a WWW em 1990, o número de hosts da Internet cresceu de poucos milhares para centenas de milhões deles.

Conforme mencionado, um endereço IPv4 consiste em apenas 32 bits. Da mesma forma, poucos endereços IP são perdidos; eles não podem ser usados devido à forma como as redes são organizadas. O número de endereços disponíveis na sua sub-rede é dois elevado à potência do número de bits, menos dois. Uma sub-rede tem, por exemplo, 2, 6 ou 14 endereços disponíveis. Para conectar 128 hosts à Internet, por exemplo, você precisa de uma sub-rede com 256 endereços IP, dos quais apenas 254 são utilizáveis, visto que são necessários dois endereços IP para a estrutura da própria sub-rede: o endereço de broadcast e o endereço de rede base.

No protocolo IPv4 atual, DHCP ou NAT (Network Address Translation — Conversão de Endereços de Rede) são os mecanismos comuns usados para contornar a grande falta

de endereços. Combinado à convenção de manter endereços públicos e privados separados por espaços, esses métodos podem certamente reduzir a falta de endereços. O problema deles está em suas configurações, trabalhosas para configurar e difíceis de manter. Para configurar um host em uma rede IPv4, é preciso que haja vários itens de endereços, como o próprio endereço IP do host, a máscara de sub-rede, o endereço de gateway e talvez um endereço de servidor de nomes. Todos esses itens precisam ser conhecidos e não podem ser derivados de outro lugar.

Com o IPv6, tanto a falta de endereços quanto as configurações complicadas passariam a ser problemas do passado. As seções a seguir oferecem mais informações sobre os aprimoramentos e benefícios trazidos pelo IPv6 e sobre a transição do protocolo antigo para o novo.

23.2.1 Vantagens

A melhoria mais importante e visível oferecida pelo novo protocolo é a expansão enorme do espaço disponível para endereços. Um endereço IPv6 é criado com valores de 128 bits em vez dos 32 bits tradicionais. Ele é capaz de fornecer 'quatrilhões' de endereços IP.

Entretanto, os endereços IPv6 não diferem de seus antecessores apenas em relação ao comprimento. Também possuem uma estrutura interna diferente, que pode conter mais informações específicas sobre os sistemas e as redes a que pertencem. Leia mais detalhes sobre eles na Seção 23.2.2, “Estrutura e tipos de endereços” (p 309).

A seguir, há uma lista de algumas outras vantagens do novo protocolo:

Configuração automática

O IPv6 torna apto o “plug and play” da rede, o que significa que um sistema recentemente configurado é integrado à rede (local) sem qualquer configuração manual. O novo host usa seu mecanismo de configuração automática para derivar seu próprio endereço a partir das informações disponibilizadas pelos roteadores vizinhos, com base em um protocolo chamado *ND* (Neighbor Discovery — descoberta de vizinho). Esse método não exige nenhuma intervenção por parte do administrador e não há necessidade de manter um servidor central para alocação de endereços; uma vantagem adicional em relação ao IPv4, cuja alocação automática de endereços exige um servidor DHCP.

Apesar disso, se houver um roteador conectado a um switch, ele deverá enviar anúncios periódicos com flags avisando os hosts de uma rede sobre como devem interagir entre si. Para obter mais informações, consulte o RFC 2462 e a página de manual de `radvd.conf(5)`, e o RFC 3315.

Mobilidade
O IPv6 torna possível a atribuição de vários endereços a uma interface de rede ao mesmo tempo. Isso permite que os usuários acessem várias redes com facilidade, algo comparável aos serviços de roaming internacional oferecidos por operadoras de telefonia celular: quando você leva seu telefone celular para o exterior, ele se registra automaticamente em um serviço estrangeiro logo que entra na área correspondente, de modo que você possa ser contatado pelo mesmo número em qualquer lugar e ligar para alguém do mesmo modo que faz em sua área de origem.

Comunicação segura
Com o IPv4, a segurança da rede é uma função adicional. O IPv6 inclui IPsec como um de seus recursos principais, permitindo que sistemas se comuniquem por um túnel seguro, para evitar a intromissão de estranhos na Internet.

Compatibilidade retroativa
De forma realista, seria impossível mudar toda a Internet de IPv4 para IPv6 de uma só vez. Portanto, é essencial que ambos os protocolos sejam capazes de coexistir na Internet, mas também em um sistema. Isso é garantido por endereços compatíveis (endereços IPv4 podem facilmente ser convertidos em endereços IPv6) e através do uso de vários túneis. Consulte a Seção 23.2.3, "Coexistência de IPv4 e IPv6" (p 314). Da mesma forma, os sistemas podem se basear em uma técnica *IP de pilha dupla* para suportar os dois protocolos ao mesmo tempo, significando que possuem duas pilhas de rede completamente separadas, de tal forma que não há interferência entre as duas versões de protocolos.

Serviços adaptados e personalizados através de Multicast
Com o IPv4, alguns serviços, como SMB, precisam transmitir seus pacotes para todos os host na rede local. O IPv6 oferece uma abordagem mais detalhada, permitindo que os servidores enviem hosts através de *multicast* — determinando um número de hosts como partes de um grupo (o que é diferente de direcionar todos os hosts através de *broadcast* ou cada host individualmente através de *unicast*). Os hosts enviados como grupos talvez dependam do aplicativo concreto. É possível enviar todos os servidores de nomes para alguns grupos predefinidos (o *grupo multicast de servidores de nomes*), por exemplo ou todos os roteadores (o *grupo multicast de todos os roteadores*).

23.2.2 Estrutura e tipos de endereços

Conforme mencionado, o protocolo IP atual está em desvantagem em relação a dois aspectos importantes: os endereços IP estão cada vez mais escassos, e a configuração de rede com manutenção de tabelas de rotina vem se tornando cada vez mais uma tarefa complexa e onerosa. O IPv6 soluciona o primeiro problema, expandindo o espaço dos endereços para 128 bits. O segundo problema é contornado com a introdução de uma estrutura hierárquica de endereços, combinada com técnicas sofisticadas para alocar endereços de rede, assim como *multihoming* (a capacidade de designar vários endereços a um dispositivo, permitindo acesso a diversas redes).

Ao utilizar o IPv6, é útil saber que há três tipos diferentes de endereços:

Unicast
: Endereços desse tipo são associados com exatamente uma interface de rede. Pacotes com esse tipo de endereço são entregues em apenas um destino. Da mesma forma, os endereços unicast são usados para transferir pacotes para hosts individuais na rede local ou na Internet.

Multicast
: Endereços desse tipo estão relacionados a um grupo de interfaces de rede. Pacotes com esse tipo de endereço são entregues a todos os destinos pertencentes ao grupo. Endereços multicast são usados, principalmente, por certos tipos de serviços de rede para se comunicarem com determinados grupos de host de forma bem direcionada.

Anycast
: Endereços desse tipo estão relacionados a um grupo de interfaces. Pacotes com esse tipo de endereço são entregues ao membro do grupo mais próximo do remetente, de acordo com os princípios do protocolo de roteamento subjacente. Endereços anycast são usados para que hosts possam descobrir mais facilmente servidores que oferecem certos serviços na área da rede determinada. Todos os servidores do mesmo tipo possuem o mesmo endereço anycast. Sempre que um host solicita um serviço, ele recebe uma resposta do servidor com o local mais próximo, conforme determinado pelo protocolo de roteamento. Caso ocorra alguma falha com esse servidor, o protocolo selecionará automaticamente o segundo servidor mais próximo ou então o terceiro e assim por diante.

Um endereço IPv6 é constituído de oito campos de quatro dígitos, cada um representando 16 bits, gravados em notação hexadecimal. Eles são separados por dois-pontos (`:`).

Quaisquer zero bytes iniciais em um determinado campo podem ser descartados, mas zeros dentro ou no final do campo não podem ser descartados. Outra convenção é a de que mais de quatro zero bytes consecutivos podem retornar como dois-pontos duplos. Entretanto, apenas um separador do tipo `::` é permitido por endereço. Esse tipo de notação reduzida é mostrado no Exemplo 23.3, “Amostra de endereço IPv6” (p 310), em que todas as três linhas representam o mesmo endereço.

Exemplo 23.3 *Amostra de endereço IPv6*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                           : 10 : 1000 : 1a4
```

Cada parte de um endereço IPv6 possui uma função definida. Os primeiros bytes formam o prefixo e especificam o tipo de endereço. A parte central é a porção do endereço na rede, mas pode não ser utilizada. O final do endereço forma a parte do host. Com o IPv6, a máscara de rede é definida indicando o comprimento do prefixo depois de uma barra no final do endereço. Um endereço, como mostrado no Exemplo 23.4, “Endereço IPv6 especificando o comprimento do prefixo” (p 310), contém as informações de que os primeiros 64 bits formam a parte da rede do endereço e que os últimos 64 formam a parte do host. Em outras palavras, `64` significa que a máscara de rede está preenchida com 64 valores de 1 bit a partir da esquerda. Da mesma forma que o IPv4, o endereço IP é combinado com E com os valores da máscara de rede, para determinar se o host está localizado na mesma sub-rede ou em outra.

Exemplo 23.4 *Endereço IPv6 especificando o comprimento do prefixo*

```
fe80::10:1000:1a4/64
```

O IPv6 conhece vários tipos de prefixos predefinidos. Alguns são mostrados na Tabela 23.4, “Vários prefixos IPv6” (p 310).

Tabela 23.4 *Vários prefixos IPv6*

Prefixo (hex)	Definição
`00`	Endereços IPv4 e endereços de compatibilidade de IPv4 sobre IPv6. Esses são usados para manter a compatibilidade com IPv4. O seu uso ainda exige um roteador capaz de converter pacotes IPv6 em pacotes IPv4. Vários endereços especiais, como

Prefixo (hex)	Definição
	o do dispositivo loopback, também possuem esse prefixo.
2 ou 3 como o primeiro dígito	Endereços unicast globais agregativos. Como no caso do IPv4, uma interface pode ser designada para fazer parte de uma determinada sub-rede. Atualmente, existem os seguintes espaços de endereço: 2001::/16 (espaço de endereço de qualidade de produção) e 2002::/16 (espaço de endereço 6to4).
fe80::/10	Endereços locais de links. Endereços com esse prefixo não devem ser roteados e, portanto, só devem ser encontrados na mesma sub-rede.
fe80::/10	Endereços locais de sites. Esses podem ser roteados, mas somente na rede da organização a que pertencem. Na verdade, eles são o equivalente IPv6 do espaço de endereço de rede privada atual, como 10.x.x.x.
ff	Esses são endereços multicast.

Um endereço unicast consiste em três componentes básicos:

Topologia pública
: A primeira parte (que também contém um dos prefixos mencionados acima) é usada para rotear pacotes através da Internet pública. Ela inclui informações sobre a empresa ou instituição que fornece o acesso à Internet.

Topologia do site
: A segunda parte contém informações de roteamento sobre a sub-rede à qual o pacote deve ser entregue.

ID de interface
: A terceira parte identifica a interface à qual o pacote deve ser entregue. Isso também permite que o MAC faça parte do endereço. Como MAC é um identificador fixo globalmente exclusivo codificado no dispositivo pelo fabricante do hardware, o procedimento de configuração é bastante simplificado. Na verdade, os primeiros 64 bits de endereço são consolidados para formar o token `EUI-64`, com os últimos 48 bits obtidos no MAC e os 24 bits restantes contendo informações especiais sobre o tipo de token. Isso também possibilita designar um token `EUI-64` a interfaces que não possuem MAC, como aquelas baseadas em PPP ou ISDN.

No topo dessa estrutura básica, o IPv6 faz distinção entre cinco tipos de endereços unicast:

`::` (não especificado)
: Esse endereço é usado pelo host como seu endereço de origem durante a primeira inicialização da interface, quando o endereço ainda não pode ser determinado por outros meios.

`::1` (loopback)
: O endereço do dispositivo loopback.

Endereços compatíveis com o IPv4
: O endereço IPv6 é formado pelo endereço IPv4 e um prefixo consistindo em 96 zero bits. Esse tipo de endereço de compatibilidade é usado para um túnel (consulte a Seção 23.2.3, “Coexistência de IPv4 e IPv6” (p 314)) para permitir que os hosts IPv4 e IPv6 se comuniquem com outros que estejam operando em um ambiente IPv4 puro.

Endereços IPv4 mapeados para IPv6
: Esse tipo de endereço especifica um endereço IPv4 puro em uma notação IPv6.

Endereços locais
: Há dois tipos de endereços para uso local:

  link-local
  : Esse tipo de endereço só pode ser usado na sub-rede local. Pacotes com endereço de origem ou de destino desse tipo não devem ser roteados para a Internet nem para outras sub-redes. Esses endereços contêm um prefixo especial (`fe80::/10`) e o ID da interface da placa de rede, com a parte do meio consistindo em zero bytes. Endereços desse tipo são usados durante a

configuração automática para se comunicarem com outros hosts pertencentes à mesma sub-rede.

site-local
: Pacotes com esse tipo de endereço podem ser roteados para outras sub-redes, mas não para a Internet mais ampla. Eles precisam permanecer dentro da própria rede da organização. Tais endereços são usados para intranets e equivalem ao espaço de endereço privado definido pelo IPv4. Eles contêm um prefixo especial (`fec0::/10`), o ID da interface e um campo de 16 bits especificando o ID da sub-rede. Novamente, o restante é preenchido com zero bytes.

Como um recurso completamente novo, introduzido com o IPv6, cada interface de rede normalmente obtém vários endereços IP, com a vantagem de que várias redes podem ser acessadas através da mesma interface. Uma dessas redes pode ser totalmente configurada automaticamente usando o MAC e um prefixo conhecido, resultando na possibilidade de todos os hosts na rede local serem encontrados assim que o IPv6 for habilitado (usando o endereço link-local). Com o MAC fazendo parte disso, qualquer endereço IP usado no mundo será exclusivo. As únicas partes variáveis do endereço são aquelas que indicam a *topologia do site* e a *topologia pública*, dependendo da rede real na qual o host estiver operando no momento.

Para que um host avance e retroceda entre duas redes diferentes ele precisa de, pelo menos, dois endereços. Um deles, o *endereço pessoal*, contém não só o ID de interface, como também um identificador da rede doméstica a que ele normalmente pertence (e o prefixo correspondente). O endereço pessoal é um endereço estático e, portanto, normalmente não se modifica. Mesmo assim, todos os pacotes destinados ao host móvel podem ser entregues a ele, independentemente de ele operar na rede doméstica ou em outro local externo. Isso é possível devido aos recursos totalmente novos introduzidos com o IPv6, como *configuração automática sem estado* e *descoberta de vizinho*. Além do endereço residencial, um host móvel obtém um ou mais endereços adicionais pertencentes às redes interurbanas com roaming. Eles são chamados endereços *care-of.* A rede doméstica tem um recurso que encaminha qualquer pacote destinado ao host quando ele está em roaming. Em um ambiente IPv6, essa tarefa é executada pelo *agente local*, que retransmite todos os pacotes destinados ao endereço residencial através de um túnel. Por outro lado, esses pacotes destinados ao endereço care-of são diretamente transferidos para o host móvel sem qualquer desvio especial.

23.2.3 Coexistência de IPv4 e IPv6

A migração de todos os hosts conectados à Internet do IPv4 para o IPv6 é um processo gradual. Os dois protocolos coexistirão durante algum tempo. A coexistência deles em um sistema é garantida onde houver uma implementação de *pilha dupla* de ambos os protocolos. Ainda resta a dúvida de como um host habilitado do IPv6 deve se comunicar com um host IPv4 e como pacotes do IPv6 devem ser transportados pelas redes atuais, que são predominantemente baseadas no IPv4. As melhores soluções oferecem endereços de compatibilidade e túnel (consulte a Seção 23.2.2, "Estrutura e tipos de endereços" (p 309)).

Os hosts IPv6 que estiverem mais ou menos isolados na rede IPv4 (mundial) podem se comunicar por túneis: os pacotes IPv6 são encapsulados como pacotes IPv4 para que sejam transmitidos por uma rede IPv4. Tal conexão entre dois hosts IPv4 é chamada de *túnel*. Para que isso ocorra, os pacotes precisam incluir o endereço de destino do IPv6 (ou o prefixo correspondente), assim como o endereço IPv4 do host remoto no destino final do túnel. Um túnel básico pode ser configurado manualmente, de acordo com um contrato entre os administradores dos hosts. Também é chamado de *túnel estático*.

Entretanto, a configuração e manutenção de túneis estáticos é normalmente muito trabalhosa para ser usada diariamente em comunicações. Portanto, o IPv6 fornece três métodos de *túneis dinâmicos*:

6over4
: Os pacotes IPv6 são automaticamente encapsulados como pacotes IPv4 e enviados por uma rede IPv4 com capacidade multicast. O IPv6 é induzido a considerar a rede inteira (Internet) como uma gigantesca rede local. Com isso, é possível determinar automaticamente o destino final do túnel IPv4. Entretanto, esse método não faz um dimensionamento muito bom e também é dificultado pelo fato de o multicast IP não ser tão difundido na Internet. Portanto, ele apenas fornece uma solução para redes corporativas ou institucionais menores, em que o multicast pode ser habilitado. As especificações para esse método estão descritas no RFC 2529.

6to4
: Com esse método, os endereços IPv4 são automaticamente gerados a partir de endereços IPv6, habilitando a comunicação de hosts IPv6 isolados através de uma rede IPv4. Entretanto, alguns problemas foram relatados no que tange à comunicação entre esses hosts IPv6 isolados e a Internet. O método está descrito no RFC 3056.

Controlador do túnel IPv6
: Esse método se baseia em servidores especiais que fornecem túneis dedicados para hosts IPv6. É descrito no RFC 3053.

23.2.4 Configurando o IPv6

Para configurar o IPv6, normalmente não é necessário fazer mudanças nas estações de trabalho individuais. O IPv6 é habilitado por padrão. Você pode desabilitá-lo durante a instalação na etapa de configuração da rede, descrita na Section “Network Configuration” (Chapter 3, *Installation with YaST*, ↑*Deployment Guide*). Para desabilitar ou habilitar o IPv6 em um sistema instalado, use o módulo *Configurações de Rede* do YaST. Na guia *Opções Globais*, marque ou desmarque a opção *Habilitar IPv6* conforme for necessário. Se desejar habilitá-lo temporariamente até a próxima reinicialização, digite `modprobe -i ipv6` enquanto `root`. Basicamente, é impossível descarregar o módulo ipv6 depois de carregado.

Devido ao conceito de configuração automática do IPv6, um endereço é designado à placa de rede na rede *link-local*. Normalmente, nenhum gerenciamento de tabela de roteamento é feito em uma estação de trabalho. Os roteadores de rede podem ser consultados pela estação de trabalho, usando o *protocolo de anúncios do roteador*, para o qual devem ser implementados um prefixo e gateways. O programa radvd pode ser usado para configurar um roteador IPv6. Esse programa informa às estações de trabalho o prefixo que deve ser usado para os endereços IPv6 e os roteadores. Outra opção é usar zebra/quagga para a configuração automática dos dois endereços e para roteamento.

Consulte a página de manual do ifcfg-tunnel (5) para obter informações sobre como configurar vários tipos de túneis usando os arquivos `/etc/sysconfig/network`.

23.2.5 Para obter mais informações

A visão geral acima não abrange totalmente o tópico do IPv6. Para obter informações mais detalhadas sobre o novo protocolo, consulte os livros e a documentação online a seguir:

http://www.ipv6.org/
: O ponto de partida para tudo relativo ao IPv6.

`http://www.ipv6day.org`
: Todas as informações necessárias para iniciar sua própria rede IPv6.

`http://www.ipv6-to-standard.org/`
: A lista de produtos habilitados para IPv6.

`http://www.bieringer.de/linux/IPv6/`
: Aqui, encontre o Linux IPv6-HOWTO e muitos links relacionados ao tópico.

RFC 2640
: Informações fundamentais do RFC sobre o IPv6.

IPv6 Essentials
: Um livro que descreve todos os aspectos importantes do tópico é o *IPv6 Essentials* de Silvia Hagen (ISBN 0-596-00125-8).

23.3 Resolução de nomes

O DNS ajuda na designação de um endereço IP a um ou mais nomes e na designação de um nome a um endereço IP. No Linux, essa conversão normalmente é executada por um tipo especial de software chamado bind. A máquina responsável por essa conversão é chamada de *servidor de nomes*. Os nomes criam um sistema hierárquico, no qual cada componente do nome é separado um ponto. A hierarquia de nomes é, entretanto, independente da hierarquia de endereços IP descrita acima.

Considere um nome completo, como `jupiter.exemplo.com`, escrito no formato `nome_de_host.domínio`. Um nome completo, denominado *FQDN* (Fully Qualified Domain Name - Nome de Domínio Totalmente Qualificado), consiste em um nome de host e um nome de domínio (`example.com`). O último também inclui o *TLD* (Top Level Domain — Domínio de Nível Superior) (`com`).

A designação TLD tornou-se bastante confusa por razões históricas. Tradicionalmente, nomes de domínio com três letras são usados nos EUA. No resto do mundo, os códigos nacionais ISO de duas letras são o padrão. Além disso, TLDs mais longos foram introduzidos em 2000, representando certas esferas de atividades (por exemplo, `.info`, `.name`, `.museum`).

No início da Internet (antes de 1990), o arquivo /etc/hosts era usado para armazenar os nomes de todas as máquinas representadas na Internet. Isso rapidamente se tornou impraticável, devido ao crescente número de computadores conectados à Internet. Por essa razão, um banco de dados descentralizado foi desenvolvido para armazenar nomes de hosts de uma forma amplamente distribuída. Esse banco de dados, semelhante ao servidor de nomes, não possui os dados pertencentes a todos os hosts na Internet já disponíveis, mas pode encaminhar solicitações a outros servidores de nomes.

A parte superior da hierarquia é ocupada pelos *servidores de nomes raiz*. Esses servidores de nomes raiz gerenciam os domínios de nível superior e são executados pelo NIC (Network Information Center). Cada servidor de nomes raiz conhece os servidores de nomes responsáveis por um determinado domínio de nível superior. Para obter informações sobre NICs de domínio superior, vá para http://www.internic.net.

O DNS pode fazer mais do que apenas resolver nomes de hosts. O servidor de nomes também distingue qual host recebe e-mails para um domínio inteiro: o *MX (servidor de correio)*.

Para sua máquina resolver um endereço IP, ela precisa pelo menos conhecer um servidor de nomes e seu respectivo endereço IP. É fácil especificar esse servidor de nomes com a ajuda do YaST. Se você tiver uma conexão de discagem por modem, talvez não precise nem mesmo configurar um servidor de nomes manualmente. O protocolo de discagem fornece o endereço do servidor de nomes enquanto a conexão é efetuada.

O protocolo whois está intimamente relacionado ao DNS. Com esse programa, é possível descobrir rapidamente o responsável por qualquer domínio especificado.

NOTA: MDNS e nomes do domínio .local

O domínio de nível superior .local é tratado como domínio link-local pelo resolver. As solicitações de DNS são enviadas como solicitações de DNS multicast, em vez de solicitações de DNS normal. Se você já usa o domínio .local em sua configuração de servidor de nomes, deverá desativar essa opção em /etc/host.conf. Para obter mais informações, consulte a página de manual host.conf.

Se desejar desativar o MDNS durante a instalação, use nomdns=1 como parâmetro de boot.

Para obter mais informações sobre DNS de multicast, consulte http://www.multicastdns.org.

23.4 Configurando uma conexão de rede com o YaST

Há muitos tipos de redes suportadas no Linux. A maioria delas usa nomes de dispositivos diferentes e os arquivos de configuração se espalham por vários locais no sistema de arquivos. Para obter uma visão geral detalhada dos aspectos da configuração manual de rede, consulte a Seção 23.6, “Configurando uma conexão de rede manualmente” (p 342).

No SUSE Linux Enterprise Desktop, em que o NetworkManager está ativo por padrão, todas as placas de rede estão configuradas. Se o NetworkManager não estiver ativo, apenas a primeira interface com link ativo (com cabo de rede conectado) será configurada automaticamente. Hardwares adicionais podem ser configurados a qualquer momento no sistema instalado. As seguintes seções descrevem a configuração de rede para todos os tipos de conexões de rede suportadas pelo SUSE Linux Enterprise Desktop.

23.4.1 Configurando a placa de rede com o YaST

Para configurar sua placa de rede wireless ou não no YaST, selecione *Dispositivos de Rede* > *Configurações de Rede*. Após iniciar o módulo, o YaST exibirá a caixa de diálogo *Configurações de Rede* com quatro guias: *Opções Globais*, *Visão Geral*, *Nome de host/DNS* e *Roteamento*.

A guia *Opções Globais* permite definir opções gerais de rede, como o uso do NetworkManager, o IPv6 e opções gerais de DHCP. Para obter mais informações, consulte a Seção 23.4.1.1, “Configurando opções globais de rede” (p 319).

A guia *Visão Geral* contém informações sobre interfaces de rede instaladas e configurações. Ela lista os nomes de todas as placas de rede detectadas corretamente. Nessa caixa de diálogo, você pode configurar manualmente novas placas, bem como remover ou mudar suas configurações. Se você quiser configurar manualmente uma placa que não foi detectada automaticamente, consulte a Seção 23.4.1.3, “Configurando

uma placa de rede não detectada” (p 326). Se você quiser mudar a configuração de uma placa que já está configurada, consulte Seção 23.4.1.2, “Mudando a configuração de uma placa de rede” (p 321).

A guia *Nome de Host/DNS* permite definir o nome de host da máquina e nomear os servidores que serão usados. Para obter mais informações, consulte Seção 23.4.1.4, “Configurando o nome do host e o DNS” (p 327).

A guia *Roteamento* é usada para a configuração do roteamento. Consulte a Seção 23.4.1.5, “Configurando o roteamento” (p 329) para obter mais informações.

Figura 23.3 *Definindo as configurações da rede*

23.4.1.1 Configurando opções globais de rede

A guia *Opções Globais* do módulo *Configurações de Rede* do YaST permite definir opções globais de rede importantes, como o uso do NetworkManager, o IPv6 e opções de cliente DHCP. Essas configurações são aplicáveis a todas as interfaces de rede.

Em *Método de Configuração da Rede*, escolha o modo como as conexões de rede são gerenciadas. Para que um applet de área de trabalho do NetworkManager gerencie as conexões de todas as interfaces, escolha *Controlado por Usuário com o NetworkManager*. Essa opção é ideal para fazer a alternância entre várias redes wireless ou não. Se você não tem um ambiente de área de trabalho (GNOME ou KDE) em execução, ou se o seu computador for um servidor Xen, um sistema virtual ou fornecer serviços de rede como DHCP ou DNS na rede em que se encontra, use o *Método Tradicional com ifup*. Se o NetworkManager for usado, o `nm-applet` deverá ser usado para configurar opções de rede, e as guias *Visão Geral*, *Nome de host/DNS* e *Roteamento* do módulo *Configurações de Rede* estarão desabilitadas. Para obter mais informações sobre o NetworkManager, consulte o Capítulo 26, *Usando o NetworkManager* (p 379).

Nas *Configurações do Protocolo IPv6*, escolha entre usar ou não o protocolo IPv6. É possível usar o IPv6 juntamente com o IPv4. Por padrão, o IPv6 fica ativado. Contudo, nas redes que não usam o protocolo IPv6, os tempos de resposta podem ser acelerados com o protocolo IPv6 desabilitado. Para desabilitar o IPv6, desmarque a opção *Habilitar IPv6*. Isso desabilita o carregamento automático do módulo de kernel do IPv6. Essa ação será aplicada após a reinicialização.

Nas *Opções do Cliente DHCP*, configure as opções do cliente DHCP. Se você quiser que o cliente DHCP peça ao servidor para sempre transmitir suas respostas, marque *Requerer Resposta a Broadcast*. Isso pode ser necessário se houver o costume de mover a sua máquina entre redes diferentes. O *Identificador de Cliente DHCP* deve ser diferente para cada cliente DHCP na mesma rede. Se ficar vazio, assumirá como padrão o endereço de hardware da interface da rede. Entretanto, se você tiver várias máquinas virtuais em execução na mesma interface de rede e, portanto, com o mesmo endereço de hardware, especifique aqui um identificador exclusivo.

O *Nome do Host a Enviar* especifica uma string usada no campo da opção de nome de host quando o dhcpcd envia mensagens ao servidor DHCP. Alguns servidores DHCP atualizam as zonas do servidor de nomes (registros diretos e reversos) de acordo com esse nome de host (DNS Dinâmico). Além disso, alguns servidores DHCP exigem que o campo da opção *Nome do Host a Enviar* contenha uma string específica nas mensagens DHCP dos clientes. Mantenha `AUTO` para enviar o nome de host atual (ou seja, o que está definido em `/etc/HOSTNAME`). Deixe o campo da opção vazio para não enviar nenhum nome de host. Se você não quiser mudar a rota padrão de acordo com as informações do DHCP, desmarque *Mudar Rota Padrão via DHCP*.

23.4.1.2 Mudando a configuração de uma placa de rede

Para mudar a configuração de uma placa de rede, selecione-a na lista de placas detectadas em *Configurações de Rede* > *Visão Geral* no YaST e clique em *Editar*. A caixa de diálogo *Configuração da Placa de Rede* é exibida, na qual é possível ajustar a configuração da placa usando as guias *Geral*, *Endereço* e *Hardware*. Para obter informações sobre a configuração de placas wireless, consulte a Seção 20.5, “Configuração com o YaST” (p 262).

Configurando endereços IP

Você pode definir o endereço IP da placa de rede ou o modo como seu endereço IP é determinado na guia *Endereço* da caixa de diálogo *Configuração da Placa de Rede*. Há suporte para endereços IPv4 e IPv6. A placa de rede pode ser *Sem Endereço IP* (útil para dispositivos de vinculação), ter um *Endereço IP Atribuído Estaticamente* (IPv4 ou IPv6) ou um *Endereço Dinâmico* atribuído por *DHCP*, *Zeroconf* ou ambos.

Ao usar um *Endereço Dinâmico*, selecione se deseja usar *Apenas DHCP Versão 4* (para IPv4), *Apenas DHCP Versão 6* (para IPv6) ou *DHCP Versões 4 e 6*.

Se possível, a primeira placa de rede com link que estiver disponível durante a instalação será configurada automaticamente para usar a configuração automática de endereço via DHCP. No SUSE Linux Enterprise Desktop, em que o NetworkManager está ativo por padrão, todas as placas de rede estão configuradas.

Também será necessário usar o DHCP se você estiver usando uma linha DSL sem nenhum IP estático atribuído pelo ISP (Internet Service Provider — Provedor de Serviços de Internet). Se você decidir usar o DHCP, configure os detalhes em *Opções do Cliente DHCP* na guia *Opções Globais* da caixa de diálogo *Configurações de Rede* do módulo de configuração de placa de rede do YaST. Especifique se o cliente DHCP deve pedir que o servidor sempre transmita suas respostas em *Requerer Resposta a Broadcast*. Essa opção pode ser necessária se a sua máquina for um cliente móvel que costuma trocar de rede. Se você tiver uma configuração de host virtual, em que hosts diferentes se comunicam pela mesma interface, será necessário um *Identificador de Cliente DHCP* para diferenciá-las.

O DHCP é uma boa opção para a configuração de clientes, mas não é a ideal para a configuração de servidores. Para definir um endereço IP estático, faça o seguinte:

1 Selecione uma placa na lista de placas detectadas na guia *Visão Geral* do módulo de configuração de placa de rede do YaST e clique em *Editar*.

2 Na guia *Endereço*, escolha *Endereço IP Atribuído Estaticamente*.

3 Digite o *Endereço IP*. Podem ser usados endereços IPv4 e IPv6. Digite a máscara de rede em *Máscara de Sub-rede*. Se for usado o endereço IPv6, use *Máscara de Sub-rede* para um comprimento do prefixo no formato `/64`.

   Como opção, você pode digitar um *Nome de Host* completo para esse endereço, que será gravado no arquivo de configuração `/etc/hosts`.

4 Clique em *Avançar*.

5 Para ativar a configuração, clique em *OK*.

Se você usa o endereço estático, os servidores de nomes e o gateway padrão não são configurados automaticamente. Para configurar servidores de nomes, proceda conforme descrito em Seção 23.4.1.4, “Configurando o nome do host e o DNS” (p 327). Para configurar um gateway, proceda conforme descrito em Seção 23.4.1.5, “Configurando o roteamento” (p 329).

Configurando álias

Um dispositivo de rede pode ter vários endereços IP chamados álias.

NOTA: álias são um recurso de compatibilidade

Esses supostos álias ou rótulos funcionam apenas com IPv4. Com IPv6, eles serão ignorados. O uso das interfaces de rede `iproute2` pode ter um ou mais endereços.

Ao usar o YaST para definir um álias para a placa de rede, faça o seguinte:

1 Selecione uma placa na lista de placas detectadas na guia *Visão Geral* do módulo de configuração de placa de rede do YaST e clique em *Editar*.

2 Na guia *Endereço* > *Endereços Adicionais*, clique em *Adicionar*.

3. Insira o *Nome de Apelido*, o *Endereço IP* e a *Máscara de Rede*. Não inclua o nome da interface no nome do álias.

4. Clique em *OK*.

5. Clique em *Avançar*.

6. Para ativar a configuração, clique em *OK*.

Mudando o nome de dispositivo e as regras de udev

É possível mudar o nome de dispositivo da placa de rede quando ela for usada. Também é possível determinar se a placa de rede deve ser identificada pelo udev usando o endereço (MAC) de hardware ou o ID do barramento. A segunda opção é preferível em grandes servidores para facilitar o intercâmbio das placas. Para definir essas opções com o YaST, faça o seguinte:

1. Selecione uma placa na lista de placas detectadas na guia *Visão Geral* do módulo Configurações de Rede do YaST e clique em *Editar*.

2. Vá até a guia *Hardware*. O nome de dispositivo atual é mostrado em *Regras do Udev*. Clique em *Mudar*.

3. Selecione se o udev deve identificar a placa por seu *Endereço MAC* ou *ID do Bus*. O endereço MAC e o ID do barramento atuais da placa são mostrados na caixa de diálogo.

4. Para mudar o nome de dispositivo, marque a opção *Mudar Nome do Dispositivo* e edite o nome.

5. Clique em *OK* e em *Avançar*.

6. Para ativar a configuração, clique em *OK*.

Mudando o driver do kernel da placa de rede

Para algumas placas de rede, pode haver vários drivers de kernel disponíveis. Se a placa já estiver configurada, o YaST permitirá selecionar um driver do Kernel para uso na lista de drivers compatíveis disponíveis. Também é possível especificar opções para o driver de kernel. Para definir essas opções com o YaST, faça o seguinte:

1 Selecione uma placa na lista de placas detectadas na guia *Visão Geral* do módulo Configurações de Rede do YaST e clique em *Editar*.

2 Vá até a guia *Hardware*.

3 Selecione o driver de kernel a ser usado em *Nome de Módulo*. Digite qualquer opção para o driver selecionado em *Opções*, usando o formato `opção=valor`. Se forem usadas mais opções, elas deverão ser separadas por espaços.

4 Clique em *OK* e em *Avançar*.

5 Para ativar a configuração, clique em *OK*.

Ativando o dispositivo de rede

Se você usa o método tradicional com ifup, poderá configurar seu dispositivo para ser iniciado em uma das seguintes situações: durante o boot, na conexão a cabo, ao detectar a placa, manualmente ou nunca. Para mudar a inicialização do dispositivo, faça o seguinte:

1 No YaST, selecione uma placa na lista de placas detectadas em *Dispositivos de Rede* > *Configurações de Rede* e clique em *Editar*.

2 Na guia *Geral*, selecione a entrada desejada em *Ativação de Dispositivo*.

   Escolha *Em Tempo de Boot* para iniciar o dispositivo durante o boot do sistema. Com a opção *Em Conexão Cabo*, a interface é monitorada quanto a qualquer conexão física existente. Com a opção *Em Hotplug*, a interface é definida tão logo fique disponível. Ela se assemelha à opção *Em Tempo de Boot*, a única diferença é que não ocorre nenhum erro quando a interface não está presente no momento do boot. Escolha *Manualmente* para controlar a interface manualmente com `ifup`. Escolha *Nunca* para não iniciar o dispositivo. A opção *Em NFSroot* se assemelha a *Em Tempo de Boot*, porém, a interface não é encerrada com o comando `rcnetwork stop`. Use-a se você estiver usando um sistema de arquivos raiz nfs ou iscsi.

3 Clique em *Avançar*.

4 Para ativar a configuração, clique em *OK*.

Geralmente, apenas o administrador do sistema pode ativar e desativar as interfaces de rede. Para que qualquer usuário seja capaz de ativar essa interface via KInternet, selecione *Habilitar Controle de Dispositivo para Usuário Não Root Via KInternet*.

Configurando o tamanho da unidade máxima de transferência

Você pode definir uma unidade máxima de transferência (MTU) para a interface. A MTU refere-se ao maior tamanho de pacote permitido, em bytes. Uma MTU maior proporciona melhor eficiência da largura de banda. No entanto, pacotes grandes podem bloquear uma interface lenta por algum tempo, aumentando a latência dos pacotes seguintes.

1. No YaST, selecione uma placa na lista de placas detectadas em *Dispositivos de Rede* > *Configurações de Rede* e clique em *Editar*.

2. Na guia *Geral*, selecione a entrada desejada na lista *Definir MTU*.

3. Clique em *Avançar*.

4. Para ativar a configuração, clique em *OK*.

Configurando o firewall

Sem precisar inserir a configuração de firewall detalhada como descrito na Section “Configuring the Firewall with YaST” (Chapter 15, *Masquerading and Firewalls*, ↑*Security Guide*), você pode determinar a configuração de firewall básica para seu dispositivo como parte da configuração dele. Proceda da seguinte maneira:

1. Abra o módulo *Dispositivos de Rede* > *Configurações de Rede* do YaST. Na guia *Visão Geral*, selecione uma placa na lista de placas detectadas e clique em *Editar*.

2. Acesse a guia *Geral* da caixa de diálogo *Configurações de Rede*.

3. Determine a zona de firewall à qual sua interface deve ser designada. As seguintes opções estão disponíveis:

   Firewall Desabilitado
      Essa opção fica disponível apenas quando o firewall está desabilitado, sem entrar em execução. Use esta opção apenas se a sua máquina pertencer a uma rede maior protegida por um firewall externo.

Zona Atribuída Automaticamente
: Essa opção fica disponível apenas quando o firewall está habilitado. O firewall está em execução e a interface é atribuída automaticamente a uma zona de firewall. Para uma interface como essa, será usada a zona que contiver a palavra-chave `any` ou a zona externa.

Zona Interna (Desprotegida)
: O firewall está em execução, mas não assegura o uso obrigatório de nenhuma regra para proteger a interface. Use esta opção se a sua máquina pertencer a uma rede maior protegida por um firewall externo. Ela também é útil para as interfaces conectadas à rede interna, quando a máquina possui mais interfaces de rede.

Zona Desmilitarizada
: Zona desmilitarizada é uma linha de defesa adicional situada na frente de uma rede interna e da Internet (hostil). Os hosts designados a essa zona podem ser acessados a partir da rede interna e a Internet, mas não podem acessar a rede interna.

Zona Externa
: O firewall está em execução nesta interface e a protege totalmente contra outros tráfegos de rede (provavelmente hostis). Ela é a opção padrão.

4 Clique em *Avançar*.

5 Ative a configuração clicando em *OK*.

23.4.1.3 Configurando uma placa de rede não detectada

Sua placa pode ser detectada incorretamente. Nesse caso, ela não será incluída na lista de placas detectadas. Se você tiver certeza de que o sistema contém um driver para sua placa, poderá configurá-la manualmente. Se for possível, configure também tipos especiais de dispositivos de rede, como ponte, ligação, TUN ou TAP. Para configurar uma placa de rede não detectada (ou um dispositivo especial), faça o seguinte:

1 Na caixa de diálogo *Dispositivos de Rede* > *Configurações de Rede* > *Visão Geral* no YaST, clique em *Adicionar*.

2 Na caixa de diálogo *Hardware*, defina o *Tipo de Dispositivo* da interface entre as opções disponíveis e o *Nome de Configuração*. Se a placa de rede for um dispositivo PCMCIA ou USB, ative a respectiva caixa de seleção e saia dessa caixa de diálogo com *Avançar*. Caso contrário, você pode definir o *Nome de Módulo* do kernel para ser usado para a placa e as respectivas *Opções*, se necessário.

   Em *Opções do Ethtool*, você pode definir as opções de `ethtool` usadas pelo `ifup` para a interface. Consulte a página de manual de `ethtool` para conhecer as opções disponíveis. Se a string opcional iniciar com um `-` (por exemplo `-K` *`nome_da_interface`* `rx on`), a segunda palavra da string será substituída pelo nome da interface atual. Caso contrário (por exemplo `autoneg off speed 10`), `ifup` precederá `-s` *`nome_da_interface`*.

3 Clique em *Avançar*.

4 Configure quaisquer opções que forem necessárias, como o endereço IP, a ativação do dispositivo ou a zona de firewall da interface nas guias *Geral*, *Endereço* e *Hardware*. Para obter mais informações sobre as opções de configuração, consulte Seção 23.4.1.2, “Mudando a configuração de uma placa de rede” (p 321).

5 Se você selecionou *Wireless* como o tipo de dispositivo da interface, configure a conexão wireless na próxima caixa de diálogo. Informações detalhadas sobre a configuração do dispositivo wireless estão disponíveis no Capítulo 20, *Rede local sem fio* (p 257).

6 Clique em *Avançar*.

7 Para ativar a nova configuração de rede, clique em *OK*.

23.4.1.4 Configurando o nome do host e o DNS

Se você não mudou a configuração da rede durante a instalação e a placa com fio já estava disponível, um nome de host foi gerado automaticamente para o seu computador e o DHCP foi ativado. O mesmo se aplica às informações de serviço de nomes de que o host necessita para se integrar a um ambiente de rede. Se o DHCP for usado para a configuração de endereços de rede, a lista de servidores de nomes de domínio será preenchida automaticamente com os dados adequados. Se uma configuração estática for preferencial, defina esses valores manualmente.

Para mudar o nome do seu computador e ajustar a lista de pesquisa do servidor de nomes, faça o seguinte:

1 Vá para a guia *Configurações de Rede* > *Nome de host/DNS* no módulo *Dispositivos de Rede* no YaST.

2 Digite o *Nome de Host* e, se necessário, o *Nome de Domínio*. O domínio é especialmente importante quando a máquina é um servidor de correio eletrônico. Observe que o nome de host é global e se aplica a todas as interfaces de rede definidas.

Se você estiver usando o DHCP para obter um endereço IP, o nome de host do seu computador será definido automaticamente pelo DHCP. Pode ser que você queira desabilitar esse comportamento ao conectar-se a outras redes, visto que elas podem atribuir nomes de host diferentes, e a mudança de nome de host em tempo de execução pode confundir a área de trabalho gráfica. Para desabilitar o uso do DHCP para obter um endereço IP, desmarque *Trocar Nome de Host via DHCP*.

Atribuir Nome de Host a IP de Loopback associa seu nome de host ao endereço IP `127.0.0.2` (loopback) em `/etc/hosts`. Trata-se de uma opção útil quando você deseja que o nome de host seja sempre resolvível, mesmo sem uma rede ativa.

3 Em *Modificar Configuração do DNS*, selecione o modo como a configuração do DNS (servidores de nomes, lista de pesquisa, o conteúdo do arquivo `/etc/resolv.conf`) é modificada.

Se a opção *Usar Política Padrão* for selecionada, a configuração será gerenciada pelo script `netconfig`, que funde os dados definidos estaticamente (com o YaST ou nos arquivos de configuração) com os dados obtidos dinamicamente (do cliente DHCP ou do NetworkManager). Essa política padrão é suficiente na maioria dos casos.

Se a opção *Apenas Manualmente* for selecionada, `netconfig` não terá permissão para modificar o arquivo `/etc/resolv.conf`. Entretanto, esse arquivo pode ser editado manualmente.

Se a opção *Política Personalizada* for selecionada, deverá ser especificada uma string de *Regra de Política Personalizada* definindo a política de fusão. A string consiste em uma lista de nomes de interface separados por vírgula, considerada como fonte válida de configurações. Além dos nomes completos de interface, também são permitidos curingas básicos para corresponder a várias interfaces. Por exemplo,

`eth* ppp?` primeiramente encontrará todas as interfaces eth, depois, todas as interfaces de ppp0 a ppp9. Existem dois valores de política especiais que indicam como aplicar as configurações estáticas definidas no arquivo `/etc/sysconfig/network/config`:

`STATIC`
: É preciso que haja a fusão das configurações estáticas com as configurações dinâmicas.

`STATIC_FALLBACK`
: As configurações estáticas são usadas apenas quando não há nenhuma configuração dinâmica disponível.

Para obter mais informações, consulte `man 8 netconfig`.

4 Digite os *Servidores de Nome* e preencha a lista *Pesquisa de Domínio*. Servidores de nomes devem ser especificados por endereços IP, como 192.168.1.116, não por nomes de host. Os nomes especificados na guia *Pesquisa de Domínio* são nomes de domínio usados para resolver nomes de host sem um domínio especificado. Se for usada mais de uma *Pesquisa de Domínio*, separe os domínios por vírgulas ou espaços.

5 Para ativar a configuração, clique em *OK*.

É possível também editar o nome de host usando o YaST da linha de comando. As mudanças feitas pelo YaST entram em vigor imediatamente (o que não acontece quando se edita o arquivo `/etc/HOSTNAME` manualmente). Para mudar o nome de host, use o seguinte comando:

```
yast dns edit hostname=hostname
```

Para mudar os servidores de nomes, use os seguintes comandos:

```
yast dns edit nameserver1=192.168.1.116

yast dns edit nameserver2=192.168.1.116

yast dns edit nameserver3=192.168.1.116
```

23.4.1.5 Configurando o roteamento

Para que sua máquina se comunique com outras máquinas e redes, é necessário fornecer informações de roteamento para que o tráfego de rede siga o caminho correto. Se o

DHCP for usado, essas informações serão fornecidas automaticamente. Se uma configuração estática for usada, esses dados deverão ser adicionados manualmente.

1 No YaST, vá para *Configurações de Rede* > *Roteamento*.

2 Digite o endereço IP do *Gateway Padrão* (IPv4 e IPv6, se necessário). O gateway padrão corresponde a todos os destinos possíveis, mas se houver qualquer outra entrada que corresponda ao endereço requerido, use-o em vez da rota padrão.

3 É possível digitar mais entradas na *Tabela de Roteamento*. Digite o endereço IP do *Destino*, o endereço IP do *Gateway* e a *Máscara de Rede*. Selecione o *Dispositivo* pelo qual será roteado o tráfego para a rede definida (o sinal de menos significa qualquer dispositivo). Para omitir qualquer um desses valores, use o sinal de menos `-`. Para digitar um gateway padrão na tabela, use `padrão` no campo *Destino*.

> **NOTA**
>
> Se forem usadas mais rotas padrão, será possível especificar a opção métrica para determinar qual rota possui a prioridade mais alta. Para especificar a opção métrica, digite `- metric` *`número`* em *Opções*. A rota com a métrica mais alta será usada como padrão. Se o dispositivo de rede for desconectado, sua rota será removida e o dispositivo seguinte será usado. Entretanto, o kernel atual não usa métrica no roteamento estático, apenas os daemons de roteamento, como multipathd, podem fazê-lo.

4 Se o sistema for um roteador, habilite a opção *Encaminhamento IP* nas *Configurações de Rede*.

5 Para ativar a configuração, clique em *OK*.

23.4.2 Modem

No Centro de Controle do YaST, acesse a configuração do modem em *Dispositivos de Rede* > *Modem*. Se o seu modem não foi detectado automaticamente, vá até a guia *Dispositivos de Modem* e abra a caixa de diálogo da configuração manual clicando em *Adicionar*. Digite a interface para a qual o modem está conectado em *Dispositivo de Modem*.

DICA: modems GPRS e CDMA

Configure os modems CDMA e GPRS suportados com o módulo *Modem* do YaST, do mesmo modo como são configurados os modems comuns.

Figura 23.4 *Configuração do modem*

Se você estiver usando um PBX, talvez precise digitar um prefixo de discagem. Normalmente, é um zero. Consulte as instruções que acompanham o PBX para descobrir. Selecione também se usará a discagem por tom ou pulso, se o alto-falante estará ligado e se o modem aguardará até detectar um tom de discagem. A última opção não deve ser habilitada se o modem estiver conectado a um intercâmbio.

Em *Detalhes*, configure a taxa de transmissão e as strings de inicialização do modem. Somente mude essas configurações se seu modem não tiver sido detectado automaticamente ou se ele requerer configurações especiais para o funcionamento da transmissão de dados. Esse é basicamente o caso dos adaptadores do terminal ISDN. Saia dessa caixa de diálogo clicando em *OK*. Para delegar o controle do modem ao

usuário comum sem permissões de root, ative *Habilitar Controle de Dispositivo para Usuário Não Root Via KInternet*. Dessa forma, um usuário sem permissões de administrador poderá ativar ou desativar uma interface. Em *Dial Prefix Expressão Regular*, especifique uma expressão regular. O *Prefixo de Discagem* no KInternet, que pode ser modificado por um usuário normal, precisa corresponder a essa expressão regular. Se esse campo for deixado vazio, o usuário não poderá configurar um *Prefixo de Discagem* diferente sem as permissões de administrador.

Na caixa de diálogo a seguir, selecione o ISP. Para escolher a partir de uma lista de ISPs predefinida operacional em seu país, selecione *País*. Ou então, clique em *Novo* para abrir uma caixa de diálogo em que você fornecerá os dados do seu ISP. Isso inclui um nome para a conexão de discagem e o ISP, assim como o login e a senha fornecidos pelo seu ISP. Habilite *Sempre Solicitar Senha* para que a senha seja solicitada sempre que você se conectar.

Na última caixa de diálogo, especifique as opções de conexão adicionais:

Discagem sob Demanda
: Se você habilitar a *Discagem sob Demanda*, defina pelo menos um servidor de nomes. Use esse recurso apenas se a sua conexão de Internet for econômica, pois existem programas que solicitam dados da Internet periodicamente.

Modificar DNS Quando Conectado
: Essa opção é habilitada por padrão, com o efeito de que o endereço do servidor de nomes é atualizado sempre que você se conectar à Internet.

Receber DNS Automaticamente
: Se o provedor não transmitir seu servidor de nomes de domínio após a conexão, desabilite essa opção e digite os dados do DNS manualmente.

Reconectar Automaticamente
: Se essa opção estiver habilitada, a conexão será restabelecida automaticamente após uma falha.

Ignorar Prompts
: Essa opção desabilita a detecção de quaisquer prompts do servidor de discagem. Se a conexão for lenta ou não funcionar, tente essa opção.

Interface Externa do Firewall
Selecionar essa opção ativa o firewall e define a interface como externa. Desse modo, você fica protegido contra ataques externos enquanto durar a sua conexão de Internet.

Tempo Ocioso (segundos)
Com essa opção, especifique um período de inatividade da rede depois do qual o modem se desconectará automaticamente.

Detalhes IP
Essa opção abre a caixa de diálogo de configuração de endereço. Se o ISP não designar um endereço IP dinâmico ao host, desabilite *Endereço IP Dinâmico* e, depois, digite o endereço IP local do host e o endereço IP remoto. Peça essa informação ao ISP. Habilite *Rota Padrão* e feche a caixa de diálogo, selecionando *OK*.

Selecionando *Avançar*, você retorna à caixa de diálogo original, que exibirá um resumo da configuração do modem. Feche essa caixa de diálogo com *OK*.

23.4.3 ISDN

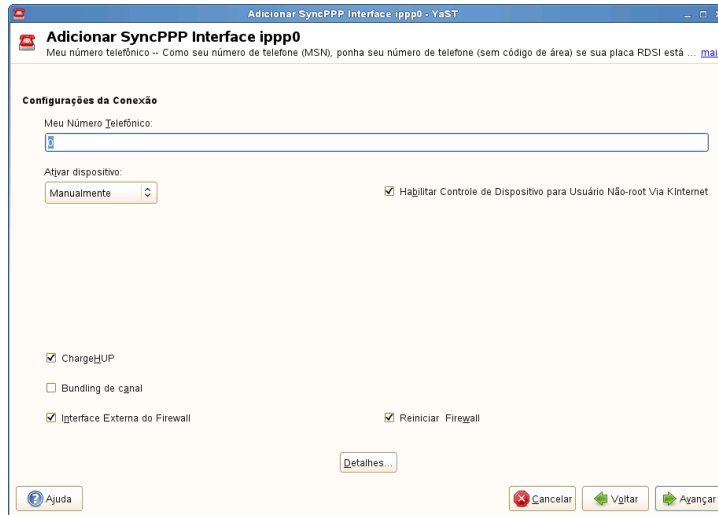
Use esse módulo para configurar uma ou várias placas ISDN para o seu sistema. Se o YaST não detectar sua placa ISDN, clique em *Adicionar* na guia *Dispositivos ISDN* e selecione a placa manualmente. É possível haver várias Interfaces, mas diversos ISPs podem ser configurados para uma única interface. Nas caixas de diálogo subsequentes, configure as opções de ISDN necessárias para o funcionamento adequado da placa.

Figura 23.5 *Configuração ISDN*

Na caixa de diálogo a seguir, mostrada na Figura 23.5, "Configuração ISDN" (p 334), selecione o protocolo a ser usado. O padrão é *Euro-ISDN (EDSS1)*, mas para intercâmbios mais antigos ou maiores, selecione *1TR6*. Se você estiver nos E.U.A., selecione *NI1*. Selecione seu país no campo relevante. O código de país correspondente aparecerá no campo próximo a ele. Por fim, forneça seu *Código de Área* e o *Prefixo de Discagem*, se necessário. Se você não quiser registrar todo o seu tráfego ISDN, desmarque a opção *Iniciar Registro ISDN*.

Ativar Dispositivo define como a interface ISDN deve ser iniciada: *Em tempo de Boot* faz o driver ISDN ser inicializado a cada boot do sistema. *Manualmente* exige que você carregue o driver do ISDN como `root` com o comando `rcisdn start`. *Em Hotplug*, usado para dispositivos PCMCIA ou USB, carrega o driver depois que o dispositivo é conectado. Ao concluir essas configurações, selecione *OK*.

Na caixa de diálogo a seguir, especifique o tipo de interface para a placa ISDN e adicione ISPs a uma interface existente. As interfaces podem ser do tipo `SyncPPP` ou `RawIP`, mas a maioria dos ISPs opera no modo `SyncPPP`, descrito abaixo.

Figura 23.6 Configuração da interface ISDN

O número a ser digitado para *Meu Número Telefônico* dependerá da sua configuração específica:

Placa ISDN conectada diretamente à saída do fone
: Uma linha ISDN padrão fornece três números telefônicos (chamados MSNs ou multiple subscriber numbers). Se o assinante pediu mais números, poderá ter até 10. Um desses MSNs precisa ser digitado aqui, mas sem o código de área. Se você digitar o número errado, o operador de fone retornará automaticamente ao primeiro MSN designado à sua linha ISDN.

Placa ISDN conectada a um PBX
: Novamente, a configuração poderá variar de acordo com o equipamento instalado:

1. PBX menores, criados para fins domésticos, normalmente usam o protocolo Euro-ISDN (EDSS1) para chamadas internas. Esses intercâmbios possuem um barramento S0 interno e usam números internos para o equipamento conectado a eles.

   Use um dos números internos como o seu MSN. Você deveria usar, pelo menos, um dos MSNs de intercâmbio habilitados para discagem direta para fora. Se não funcionar, tente um único zero. Para obter mais informações, consulte a documentação fornecida com a central telefônica.

2. Centrais telefônicas maiores, criadas para empresas, normalmente usam o protocolo 1TR6 para chamadas internas. Seus MSNs são chamados EAZ e, geralmente, correspondem ao número de discagem direta. Para a configuração no Linux, deverá ser suficiente digitar o último dígito de EAZ. Como última opção, tente cada um dos dígitos de 1 a 9.

Para que a conexão seja encerrada pouco antes de terminar a próxima unidade de carga, habilite *ChargeHUP*. Entretanto, lembre-se de que talvez não funcione com todos os ISPs. Você também pode habilitar o agrupamento de canais (multilink PPP) selecionando a opção correspondente. Por fim, você pode habilitar o firewall para o link selecionando *Interface Externa do Firewall* e *Reiniciar Firewall*. Para habilitar o usuário comum, sem permissões de administrador, a ativar ou desativar a interface, selecione *Habilitar Controle de Dispositivo para Usuário Não Root Via KInternet*.

Detalhes abre uma caixa de diálogo em que se implementa esquemas de conexão mais complexos, não relevantes para usuários domésticos comuns. Saia da caixa de diálogo *Detalhes* selecionando *OK*.

Na caixa de diálogo seguinte, ajuste as configurações de endereços IP. Se o provedor não tiver fornecido um IP estático, selecione *Endereço IP Dinâmico*. Caso contrário, use os campos fornecidos para digitar o endereço IP local e o remoto do seu host, de acordo com as especificações do ISP. Se a interface for a rota padrão para a Internet, selecione *Rota Padrão*. Cada host só pode ter uma interface configurada como a rota padrão. Saia dessa caixa de diálogo selecionando *Avançar*.

A caixa de diálogo a seguir permite que você defina seu país e selecione um ISP. Os ISPs incluídos na lista são apenas provedores do tipo chamada-por-chamada. Se seu ISP não estiver na lista, selecione *Novo*. A caixa de diálogo *Parâmetros do Provedor* será aberta para que você digite todos os detalhes do seu ISP. Ao digitar o número telefônico, não inclua espaços vazios nem vírgulas entre os dígitos. Por fim, digite seu login e senha, conforme fornecido pelo ISP. Ao terminar, selecione *Avançar*.

Para usar *Discagem sob Demanda* em uma estação de trabalho independente, especifique também o servidor de nomes (servidor DNS). A maioria dos ISPs suporta DNS dinâmico, o que significa que o endereço IP de um servidor de nomes é enviado pelo ISP toda vez que você se conecta. Entretanto, para uma única estação de trabalho, é preciso fornecer um endereço marcador, como `192.168.22.99`. Se o ISP não suportar um DNS dinâmico, especifique os endereços IP do servidor de nomes do ISP. Se desejar, especifique um tempo de espera para a conexão — o período de inatividade da rede (em segundos) após o qual a conexão deve ser automaticamente encerrada. Confirme

as configurações com *Avançar*. O YaST exibe um resumo das interfaces configuradas. Para ativar essas configurações, selecione *OK*.

23.4.4 Modem a cabo

Em alguns países, é comum acessar a Internet por rede de TV a cabo. O assinante de TV a cabo normalmente recebe um modem, que é conectado à saída do cabo da TV em uma ponta e à placa de rede do computador na outra (usando um cabo de par trançado 10Base-TG). O modem a cabo então fornece uma conexão dedicada à Internet com um endereço IP fixo.

Dependendo as instruções fornecidas pelo seu ISP, ao configurar a placa de rede, selecione *Endereço Dinâmico* ou *Endereço IP Atribuído Estaticamente*. A maioria dos provedores usa atualmente o DHCP. Um endereço IP estático frequentemente vem como parte de uma conta comercial especial.

23.4.5 DSL

Para configurar o dispositivo DSL, selecione o módulo *DSL* na seção *Dispositivos de Rede* do YaST. O módulo YaST consiste em várias caixas de diálogo nas quais configura-se os parâmetros de links DSL com base em um dos seguintes protocolos:

- PPPoE (PPP sobre Ethernet)
- PPPoATM (PPP sobre ATM)
- CAPI para ADSL (Placas Fritz)
- PPTP (Point-to-Point Tunneling Protocol) — Áustria

Na guia *Dispositivos DSL* da caixa de diálogo *Resumo de Configuração DSL*, há uma lista de dispositivos DSL instalados. Para mudar a configuração de um dispositivo DSL, selecione-o na lista e clique em *Editar*. Se você clicar em *Adicionar*, poderá configurar manualmente um novo dispositivo DSL.

A configuração de uma conexão DSL baseada em PPPoE ou PPTP exige que a placa de rede correspondente esteja configurada de forma correta. Se isso ainda não foi feito, primeiro configure a placa, selecionando *Configurar Placas de Rede* (consulte a Seção 23.4.1, “Configurando a placa de rede com o YaST” (p 318)). No caso de um link

DSL, os endereços podem ser atribuídos automaticamente, mas não via DHCP, e é por isso que você não deve habilitar a opção *Endereço Dinâmico*. Em vez disso, digite um endereço estático simulado para a interface, como `192.168.22.1`. Em *Máscara de Sub-rede*, digite `255.255.255.0`. Se estiver configurando uma estação de trabalho independente, deixe a opção *Gateway Padrão* vazia.

DICA

Os valores em *Endereço IP* e *Máscara de Sub-rede* são apenas marcadores. Eles são necessários apenas para inicializar a placa de rede e não representam o link DSL.

Na primeira caixa de diálogo de configuração do DSL (consulte a Figura 23.7, "Configuração DSL" (p 339)), selecione o *Modo PPP* e a *Placa Ethernet* à qual se conecta o modem DSL (na maioria dos casos é `eth0`). Em seguida, use *Ativar Dispositivo* para especificar se o link DSL deve ser estabelecido durante o processo de boot. Clique em *Habilitar Controle de Dispositivo para Usuário Não Root Via KInternet* para autorizar o usuário comum, sem permissões de root, a ativar ou desativar a interface com KInternet.

Na caixa de diálogo seguinte, selecione o seu país e escolha um dos ISPs que operam na região. Os detalhes de quaisquer caixas de diálogo subsequentes da configuração DSL dependem das opções configuradas até agora. É por essa razão que eles são apenas rapidamente mencionados nos parágrafos a seguir. Para obter os detalhes sobre as opções disponíveis, leia a ajuda detalhada disponível nas caixas de diálogo.

Figura 23.7 Configuração DSL

Para usar *Discagem sob Demanda* em uma estação de trabalho independente, especifique também o servidor de nomes (servidor DNS). A maioria dos ISPs suporta DNS dinâmico. O endereço IP de um servidor de nomes é enviado pelo ISP toda vez que você estabelece conexão. Entretanto, para uma única estação de trabalho, é preciso fornecer um endereço marcador, como `192.168.22.99`. Se o ISP não suportar um DNS dinâmico, especifique o endereço IP do servidor de nomes fornecido pelo ISP.

Tempo Ocioso (em segundos) define um período de inatividade da rede depois do qual a conexão é encerrada automaticamente. Um valor de tempo de espera razoável fica entre 60 e 300 segundos. Se a opção *Discagem sob Demanda* estiver desabilitada, talvez seja útil configurar o tempo de espera como zero para evitar um desligamento automático.

A configuração do T-DSL é muito parecida com a do DSL. Basta selecionar *T-Online* como seu provedor e o YaST abrirá a caixa de diálogo de configuração do T-DSL. Nessa caixa de diálogo, forneça algumas informações adicionais necessárias para T-

DSL: o ID da linha, o número T-Online, o código do usuário e a senha. Tudo isso deve estar incluído nas informações que você recebeu após se inscrever no T-DSL.

23.5 NetworkManager

O NetworkManager é a solução ideal para laptops e outros computadores portáteis. Com o NetworkManager, não é necessário preocupar-se em configurar interfaces de rede e alternar entre redes quando você estiver em trânsito.

23.5.1 NetworkManager e ifup

Entretanto, como o NetworkManager não é uma solução adequada para todos os casos, você ainda pode escolher entre o método tradicional de gerenciamento de conexões de rede (ifup) e o NetworkManager. Para gerenciar sua conexão de rede com o NetworkManager, habilite-o no módulo Configurações de Rede do YaST, conforme descrito na Seção 26.2, "Habilitando ou desabilitando o NetworkManager" (p 380), e configure suas conexões de rede com o NetworkManager. Para ver uma lista dos casos de uso e uma descrição detalhada de como configurar e usar o NetworkManager, consulte o Capítulo 26, *Usando o NetworkManager* (p 379).

Veja algumas diferenças entre o ifup e o NetworkManager:

Privilégios de `root`

Se você usa o NetworkManager para configurar a rede, poderá alternar, parar ou iniciar com facilidade a conexão de rede, a qualquer momento, de dentro do ambiente de área de trabalho usando um applet. O NetworkManager também permite mudar e configurar conexões de placa wireless sem exigir privilégios de `root`. Por esse motivo, o NetworkManager é a solução ideal para uma estação de trabalho móvel.

A configuração tradicional com o ifup também oferece algumas maneiras de alternar, parar ou iniciar a conexão com ou sem a intervenção do usuário, como em dispositivos gerenciados pelo usuário. No entanto, privilégios de `root` sempre são exigidos para mudar ou configurar um dispositivo de rede. Isso normalmente é um problema para a computação móvel, na qual não é possível pré-configurar todas as possibilidades de conexão.

Tipos de conexões de rede

Tanto a configuração tradicional quanto o NetworkManager podem administrar as conexões com uma rede wireless (com acesso via WEP, WPA-PSK e WPA-Enterprise) e redes com fio, usando a configuração DHCP e estática. Eles também suportam a conexão por discagem, DSL e VPN. Com o NetworkManager, é possível também conectar um modem de banda larga móvel (3G), o que não é possível na configuração tradicional.

O NetworkManager tenta manter o computador conectado o tempo todo usando a melhor conexão disponível. Se o cabo da rede for desconectado por acidente, ele tentará reconectar. Ele é capaz de localizar a rede que tiver a melhor intensidade de sinal na lista de conexões wireless e usá-la automaticamente para uma conexão. Para obter a mesma funcionalidade com o ifup, é necessário um grande esforço de configuração.

23.5.2 Funcionalidade do NetworkManager e arquivos de configuração

As configurações individuais de conexão de rede criadas com o NetworkManager são armazenadas em perfis de configuração. As conexões do *sistema* configuradas com o NetworkManager ou o YaST são gravadas em `/etc/networkmanager/system-connections/*` ou em `/etc/sysconfig/network/ifcfg-*`. Qualquer conexão definida pelo usuário é armazenada no GConf, para o GNOME, ou em `$HOME/.kde4/share/apps/networkmanagement/*`, para o KDE.

Caso não haja nenhum perfil configurado, o NetworkManager criará um automaticamente com o nome `Auto $INTERFACE-NAME`. Isso é uma tentativa de fazer funcionar sem qualquer configuração para tantos casos quanto forem possíveis (com segurança). Se os perfis criados automaticamente não atenderem às suas necessidades, use as caixas de diálogo de configuração da conexão de rede, fornecidas pelo KDE ou pelo GNOME, para modificá-los conforme desejado. Para obter mais informações, consulte a Seção 26.3, “Configurando conexões de rede” (p 381).

23.5.3 Controlando e bloqueando recursos do NetworkManager

Em máquinas administradas centralmente, determinados recursos do NetworkManager poderão ser controlados ou desabilitados com o PolicyKit, por exemplo, se um usuário tiver permissão para modificar as conexões definidas pelo administrador ou para definir suas próprias configurações de rede. Para ver ou mudar as respectivas políticas do NetworkManager, inicie a ferramenta gráfica *Autorizações* para o PolicyKit. Na árvore do lado esquerdo, elas se encontram abaixo da entrada *network-manager-settings*. Para ver uma introdução sobre o PolicyKit e detalhes de como usá-lo, consulte o Chapter 9, *PolicyKit* (↑*Security Guide*).

23.6 Configurando uma conexão de rede manualmente

A configuração manual do software de rede deve ser sempre a última alternativa. É recomendável usar o YaST. Entretanto, essas informações de base sobre a configuração de rede também podem ajudar você na utilização do YaST.

Quando o Kernel detecta uma placa de rede e cria uma interface de rede correspondente, ele atribui um nome de dispositivo de acordo com a ordem de descoberta de dispositivos ou a ordem de carregamento dos módulos do Kernel. Os nomes de dispositivos padrão do Kernel são previsíveis apenas em ambientes de hardware muito simples ou altamente controlados. Os sistemas que permitem adicionar ou remover hardware durante o tempo de execução ou que suportam a configuração automática de dispositivos não podem contar com nomes estáveis de dispositivos de rede atribuídos pelo Kernel durante as reinicializações.

Entretanto, todas as ferramentas de configuração do sistema contam com nomes de interface persistentes. Esse problema é solucionado pelo udev. O gerador de rede persistente udev (`/lib/udev/rules.d/75-persistent-net-generator.rules`) gera uma regra que corresponde ao hardware (usando seu endereço de hardware por padrão) e atribui uma interface exclusiva persistente ao hardware. O banco de dados de interfaces de rede do udev fica armazenado no arquivo `/etc/udev/rules.d/70-persistent-net.rules`. Todas as linhas do arquivo descrevem uma interface de rede e especifique seu nome persistente. Os administradores de sistema

podem mudar os nomes atribuídos editando as entradas `NAME=""`. As regras persistentes também podem ser modificadas por meio do YaST.

A Tabela 23.5, "Scripts de configuração de rede manual" (p 343) resume os scripts mais importantes envolvidos na configuração de rede.

Tabela 23.5 *Scripts de configuração de rede manual*

Comando	Função
`ifup, ifdown, ifstatus`	Os scripts `if` iniciam ou param interfaces de rede ou retornam o status da interface especificada. Para obter mais informações, consulte a página de manual `ifup`.
`rcnetwork`	O script `rcnetwork` pode ser usado para iniciar, parar ou reiniciar todas as interfaces de rede (ou apenas uma específica). Use `rcnetwork stop` para parar, `rcnetwork start` para iniciar e `rcnetwork restart` para reiniciar interfaces de rede. Se você quiser parar, iniciar ou reiniciar apenas uma interface, use o comando seguido pelo nome da interface, por exemplo, `rcnetwork restart eth0`. O comando `rcnetwork status` exibe o estado das interfaces, seus endereços IP e indica se há um cliente DHCP em execução. Com `rcnetwork stop-all-dhcp-clients` e `rcnetwork restart-all-dhcp-clients`, você pode parar ou reiniciar clientes DHCP em execução nas interfaces de rede.

Para obter mais informações sobre o udev e os nomes de dispositivo persistentes, consulte o Capítulo 16, *Gerenciamento dinâmico de dispositivos do Kernel com `udev`* (p 209).

23.6.1 Arquivos de configuração

Esta seção fornece uma visão geral dos arquivos de configuração de rede e explica sua finalidade e formato usado.

23.6.1.1 /etc/sysconfig/network/ifcfg-*

Esses arquivos contêm as configurações de interfaces de rede. Eles incluem informações, como o modo de início e o endereço IP. Os parâmetros possíveis são descritos na página de manual de `ifup`. Além disso, a maioria das variáveis do arquivo `dhcp` poderá ser usada nos arquivos `ifcfg-*` se uma configuração geral for usada para apenas uma interface. Entretanto, a maioria das variáveis de `/etc/sysconfig/network/config` é global e não pode ser anulada em arquivos ifcfg. Por exemplo, as variáveis `NETWORKMANAGER` ou `NETCONFIG_*` são globais.

Para saber sobre o `ifcfg.template`, consulte a Seção 23.6.1.2, "`/etc/sysconfig/network/config` e `/etc/sysconfig/network/dhcp`" (p 344).

23.6.1.2 /etc/sysconfig/network/config e /etc/sysconfig/network/dhcp

O arquivo `config` contém configurações gerais para o comportamento de `ifup`, `ifdown` e `ifstatus`. `dhcp` contém configurações para DHCP. As variáveis em ambos os arquivos de configuração são comentadas. Algumas das variáveis de `/etc/sysconfig/network/config` também podem ser usadas nos arquivos `ifcfg-*`, nos quais recebem prioridade mais alta. O arquivo `/etc/sysconfig/network/ifcfg.template` lista as variáveis que podem ser especificadas para cada interface. Entretanto, a maioria das variáveis de `/etc/sysconfig/network/config` é global e não pode ser anulada em arquivos ifcfg. Por exemplo, as variáveis `NETWORKMANAGER` ou `NETCONFIG_*` são globais.

23.6.1.3 /etc/sysconfig/network/routes e /etc/sysconfig/network/ifroute-*

O roteamento estático dos pacotes TCP/IP é determinado aqui. Todas as rotas estáticas requeridas pelas várias tarefas do sistema podem ser digitadas no arquivo `/etc/sysconfig/network/routes` file: rotas para um host, rotas para um host via gateway e rotas para uma rede. Para cada interface que precisa de roteamento individual, defina um arquivo de configuração adicional: `/etc/sysconfig/network/ifroute-*`. Substitua `*` pelo nome da interface. As entradas nos arquivos de configuração de roteamento terão esta aparência:

```
# Destination     Dummy/Gateway     Netmask            Device
#
127.0.0.0         0.0.0.0           255.255.255.0      lo
204.127.235.0     0.0.0.0           255.255.255.0      eth0
default           204.127.235.41    0.0.0.0            eth0
207.68.156.51     207.68.145.45     255.255.255.255    eth1
192.168.0.0       207.68.156.51     255.255.0.0        eth1
```

O destino da rota está na primeira coluna. Essa coluna pode conter o endereço IP de uma rede ou host ou, no caso de servidores de nomes *acessíveis*, a rede ou o nome completo do host.

A segunda coluna contém o gateway padrão ou um gateway por meio do qual um host ou uma rede podem ser acessados. A terceira coluna contém a máscara de rede para redes ou hosts atrás de um gateway. Por exemplo, a máscara em `255.255.255.255` para um host atrás de um gateway.

A quarta coluna só é relevante para redes conectadas ao host local, como loopback, Ethernet, ISDN, PPP e dispositivo simulado. O nome do dispositivo deve ser digitado aqui.

Uma quinta coluna (opcional) pode ser usada para especificar o tipo de uma rota. As colunas desnecessárias devem conter um sinal de subtração − para garantir que o analisador interpretará o comando corretamente. Para obter mais detalhes, consulte a página de manual `routes(5)`.

O formato unificado para IPv4 e IPv6 agora tem a seguinte aparência:

```
prefix/lengthgateway -            [interface]
```

E o chamado formato de compatibilidade tem esta aparência:

```
prefixgatewaylength       [interface]
```

Para IPv4 ainda pode-se usar o antigo formato com máscara de rede:

```
ipv4-networkgatewayipv4-netmask [interface]
```

Os exemplos seguintes são equivalentes:

```
2001:db8:abba:cafe::/64 2001:db8:abba:cafe::dead  -             eth0
208.77.188.0/24         208.77.188.166            -             eth0

2001:db8:abba:cafe::    2001:db8:abba:cafe::dead 64             eth0
208.77.188.0            208.77.188.166           24             eth0

208.77.188.0            208.77.188.166           255.255.255.0 eth0
```

23.6.1.4 /etc/resolv.conf

O domínio ao qual o host pertence é especificado neste arquivo (palavra-chave `search`). Também está listado o status do endereço do servidor de nomes para acesso (palavra-chave `nameserver`). Vários nomes de domínio podem ser especificados no arquivo. Durante a resolução de um nome incompleto, uma tentativa de gerar um nome será feita, anexando as entradas de `pesquisa` individuais. Vários servidores de nomes podem ser especificados em várias linhas, cada uma delas começando com `nameserver`. Comentários são precedidos pelo sinal `#`. O Exemplo 23.5, “/etc/resolv.conf” (p 347) exemplifica como pode ser a aparência do `/etc/resolv.conf`.

Entretanto, o `/etc/resolv.conf` não deve ser editado manualmente. Isso porque ele é gerado pelo script `netconfig`. Para definir configurações DNS estáticas sem usar o YaST, edite as variáveis apropriadas manualmente no arquivo `/etc/sysconfig/network/config`:

`NETCONFIG_DNS_STATIC_SEARCHLIST`
: lista de nomes de domínio DNS usada para pesquisa de nome de host

`NETCONFIG_DNS_STATIC_SERVERS`
: lista de endereços IP de servidor de nomes usada para pesquisa de nome de host

`NETCONFIG_DNS_FORWARDER`
: define o nome do forwarder de DNS que precisa ser configurado

Para desabilitar a configuração do DNS usando o netconfig, defina `NETCONFIG_DNS_POLICY=''`. Para obter mais informações sobre o `netconfig`, consulte `man 8 netconfig`.

***Exemplo 23.5** /etc/resolv.conf*

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as name server
nameserver 192.168.1.116
```

23.6.1.5 /sbin/netconfig

O `netconfig` é uma ferramenta modular destinada a gerenciar configurações de rede adicionais. Ele funde as configurações definidas estaticamente com as configurações fornecidas pelos mecanismos de configuração automática, como DHCP ou PPP, de acordo com uma política predefinida. As mudanças necessárias são aplicadas ao sistema chamando-se os módulos do netconfig responsáveis pela modificação de um arquivo de configuração e pela reinicialização de um serviço ou uma ação semelhante.

O `netconfig` reconhece três ações principais. Os comandos `netconfig modify` e `netconfig remove` são usados por daemons, como DHCP ou PPP, para fornecer ou remover configurações do netconfig. Apenas o comando `netconfig update` está disponível para o usuário:

`modify`
: O comando `netconfig modify` modifica as configurações dinâmicas específicas de interface e serviço, além de atualizar a configuração da rede. O netconfig lê as configurações da entrada padrão ou de um arquivo especificado pela opção `--lease-file` *`nome_de_arquivo`* e as armazena internamente até a próxima reinicialização do sistema (ou a próxima ação modify ou remove). As configurações que já existirem para a mesma combinação de interface e serviço serão sobregravadas. A interface é especificada pelo parâmetro `-i` *`nome_da_interface`*. O serviço é especificado pelo parâmetro `-s` *`nome_do_serviço`*.

`remove`
: O comando `netconfig remove` remove as configurações dinâmicas fornecidas por uma ação modificadora para a combinação de interface e serviço especificada, além de atualizar a configuração da rede. A interface é especificada pelo parâmetro

-i *nome_da_interface*. O serviço é especificado pelo parâmetro -s *nome_do_serviço*.

update
: O comando netconfig update atualiza a configuração da rede usando as configurações atuais. Isso é útil quando a política ou a configuração estática é mudada. Use o parâmetro -m *tipo_de_módulo* se desejar atualizar apenas um serviço especificado (dns,nis ou ntp).

A política do netconfig e as configurações estáticas são definidas manualmente ou por meio do YaST no arquivo /etc/sysconfig/network/config. As configurações dinâmicas fornecidas pelas ferramentas de configuração automática, como DHCP ou PPP, são entregues diretamente por essas ferramentas com as ações netconfig modify e netconfig remove. O NetworkManager também usa as ações netconfig modify e netconfig remove. Quando o NetworkManager está habilitado, o netconfig (no modo de política auto) usa apenas as configurações do NetworkManager, ignorando as configurações de qualquer outra interface configurada pelo método tradicional ifup. Se o NetworkManager não fornecer nenhuma configuração, as configurações estáticas serão usadas como fallback. Não há suporte para a utilização mista do NetworkManager nem para o método tradicional ifup.

Para obter mais informações sobre o netconfig, consulte man 8 netconfig.

23.6.1.6 /etc/hosts

Nesse arquivo, mostrado no Exemplo 23.6, "/etc/hosts" (p 348), os endereços IP são designados a nomes de host. Se nenhum servidor de nomes for implementado, todos os hosts nos quais uma conexão IP for configurada precisarão ser listados aqui. Para cada host, digite uma linha no arquivo com o endereço IP, o nome completo do host e o nome de host. O endereço IP precisa estar no início da linha e as entradas separadas por espaços vazios e guias. Comentários são sempre precedidos pelo sinal #.

***Exemplo 23.6** /etc/hosts*

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

23.6.1.7 /etc/networks

Aqui, os nomes de rede são convertidos em endereços de rede. O formato é semelhante ao do arquivo `hosts`, exceto que os nomes de rede precedem os endereços. Consulte o Exemplo 23.7, "`/etc/networks`" (p 349).

Exemplo 23.7 */etc/networks*

```
loopback     127.0.0.0
localnet     192.168.0.0
```

23.6.1.8 /etc/host.conf

Resolução de nomes — a conversão de nomes de host e de rede através da biblioteca *resolver* é controlada por esse arquivo. Esse arquivo é usado somente para programas vinculados a libc4 ou libc5. Para programas glibc atuais, consulte as configurações em `/etc/nsswitch.conf`. Um parâmetro precisa estar sempre independente em sua própria linha. Comentários são precedidos pelo sinal `#`. A Tabela 23.6, "Parâmetros para /etc/host.conf" (p 349) mostra os parâmetros disponíveis. Uma amostra de `/etc/host.conf` é mostrada no Exemplo 23.8, "`/etc/host.conf`" (p 350).

Tabela 23.6 *Parâmetros para /etc/host.conf*

order *hosts*, *bind*	Especifica em que ordem os serviços são acessados para a resolução de nomes. Os argumentos disponíveis são (separados por espaços vazios ou vírgulas):
	hosts: pesquisa o arquivo `/etc/hosts`
	bind: acessa um servidor de nomes
	nis: usa o NIS
multi *on*/*off*	Define se um host digitado em `/etc/hosts` pode ter vários endereços IP.

nospoof *on* spoofalert *on*/*off*	Esses parâmetros influenciam o *spoof* do servidor de nomes, mas não exercem qualquer influência na configuração da rede.
trim *domainname*	O nome de domínio especificado é separado do nome de host depois da resolução do nome de host (desde que o nome de host inclua o nome de domínio). Essa opção é útil apenas quando os nomes do domínio local estão no arquivo `/etc/hosts`, mas ainda devem ser reconhecidos com os nomes de domínio anexados.

***Exemplo 23.8** /etc/host.conf*

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

23.6.1.9 /etc/nsswitch.conf

O lançamento do GNU C Library 2.0 foi acompanhado pelo lançamento do *NSS* (Name Service Switch). Consulte a página de manual do `nsswitch.conf(5)` e *The GNU C Library Reference Manual* (Manual de Referência da Biblioteca GNU C) para obter mais detalhes.

A ordem das consultas é definida no arquivo `/etc/nsswitch.conf`. Uma amostra do `nsswitch.conf` é mostrada no Exemplo 23.9, "`/etc/nsswitch .conf`" (p 350). Comentários são precedidos pelo sinal `#`. Nesse exemplo, a entrada no banco de dados `hosts` significa que uma solicitação foi enviada para `/etc/hosts` (`arquivos`) através do DNS.

***Exemplo 23.9** /etc/nsswitch.conf*

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns
```

```
services:   db files
protocols:  db files
rpc:        files
ethers:     files
netmasks:   files
netgroup:   files nis
publickey:  files

bootparams: files
automount:  files nis
aliases:    files nis
shadow:     compat
```

Os “bancos de dados” disponíveis em NSS estão listados na Tabela 23.7, “Bancos de dados disponíveis por /etc/nsswitch.conf” (p 351). As opções de configuração para bancos de dados NSS estão listadas na Tabela 23.8, “Opções de configuração para bancos de dados “NSS”” (p 352).

***Tabela 23.7** Bancos de dados disponíveis por /etc/nsswitch.conf*

`aliases`	Álias de correio implementados por `sendmail`; consulte `man 5 aliases`.
`ethers`	Endereços de Ethernet.
`netmasks`	Lista de redes e suas máscaras de sub-rede. Apenas necessário quando se usa sub-redes.
`group`	Para grupos de usuários usados por `getgrent`. Consulte também a página de manual para `group`.
`hosts`	Para nomes de hosts e endereços IP, usados por `gethostbyname` e funções similares.
`netgroup`	Listas de usuários e hosts válidos na rede com a finalidade de controlar

	permissões de acesso, consulte a página de manual do `netgroup(5)`.
`networks`	Nomes e endereços de redes, usados por `getnetent`.
`publickey`	Chaves públicas e secretas de Secure_RPC usadas pelo NFS e NIS+.
`passwd`	Senhas de usuários, usadas por `getpwent`; consulte a página de manual do `passwd(5)`.
`protocols`	Protocolos de rede, usados por `getprotoent`; consulte a página de manual do `protocols(5)`.
`rpc`	Nomes e endereços de RPC (Remote Procedure Call) usados por `getrpcbyname` e funções similares.
`services`	Serviços de rede, usados por `getservent`.
`shadow`	Senhas transitórias de usuários, usadas por `getspnam`; consulte a página de manual do `shadow(5)`.

Tabela 23.8 *Opções de configuração para bancos de dados "NSS"*

`files`	arquivos de acesso direto, por exemplo, `/etc/aliases`
`db`	acesso através de um banco de dados
`nis`, `nisplus`	NIS, consulte também o Chapter 3, *Using NIS* (↑*Security Guide*)

dns	só pode ser usada como extensão de hosts e networks
compat	só pode ser usada como extensão de passwd, shadow e group

23.6.1.10 /etc/nscd.conf

Esse arquivo é usado para configurar o nscd (name service cache daemon). Consulte as páginas de manual de `nscd(8)` e `nscd.conf(5)`. Por padrão, as entradas do sistema de `passwd` e `groups` são armazenadas em cache pelo nscd. Isso é importante para o desempenho de serviços de diretório, como NIS e LDAP, pois, caso contrário, a conexão de rede precisaria ser usada para cada acesso a nomes ou grupos. `hosts` não é armazenado em cache por padrão, porque o mecanismo no nscd para armazenar hosts em cache impede o sistema local de confiar em verificações de pesquisa forward e reverse. Em vez de solicitar ao nscd para armazenar nomes em cache, configure um servidor DNS para armazenamento em cache.

Se o armazenamento em cache de `passwd` estiver ativado, normalmente levará quinze segundos para que um usuário local recentemente adicionado seja reconhecido. Reduza esse tempo de espera reiniciando o nscd com o comando `rcnscd restart`.

23.6.1.11 /etc/HOSTNAME

Contém o nome completo do host com o nome de domínio anexado. Esse arquivo é lido por vários scripts durante o boot da máquina. Ele deve conter apenas uma linha (na qual o nome de host é definido).

23.6.2 Testando a configuração

Antes de gravar sua configuração nos arquivos de configuração, você pode testá-la. Para definir uma configuração de teste, use o comando `ip`. Para testar a conexão, use o comando `ping`. As antigas ferramentas de configuração `ifconfig` e `route` também estão disponíveis.

Os comandos `ip`, `ifconfig` e `route` mudam a configuração da rede diretamente sem gravá-la no arquivo de configuração. A menos que você insira a configuração nos arquivos de configuração corretos, a configuração de rede mudada será perdida na reinicialização.

23.6.2.1 Configurando uma interface de rede com ip

`ip` é uma ferramenta para mostrar e configurar dispositivos de rede, roteamentos, roteamento de políticas e túneis.

`ip` é uma ferramenta muito complexa. Sua sintaxe comum é `ip` *`opções objeto comando`*. Você pode trabalhar com os seguintes objetos:

link
: Este objeto representa um dispositivo de rede.

address
: Este objeto representa o endereço IP do dispositivo.

neighbor
: Este objeto representa uma entrada de cache ARP ou NDISC.

route
: Este objeto representa a entrada da tabela de roteamento.

rule
: Este objeto representa uma regra no banco de dados de políticas de roteamento.

maddress
: Este objeto representa um endereço multicast.

mroute
: Este objeto representa uma entrada de cache de roteamento multicast.

tunnel
: Este objeto representa um túnel sobre IP.

Se nenhum comando for fornecido, será usado o comando padrão (normalmente `list`).

Mude o estado de um dispositivo com o comando `ip link set` *`nome_do_dispositivo comando`*. Por exemplo, para desativar o dispositivo eth0, digite `ip link set eth0 down`. Para ativá-lo novamente, use `ip link set eth0 up`.

Após ativar um dispositivo, você poderá configurá-lo. Para definir o endereço IP, use `ip addr add` *`endereço_ip`* `+ dev` *`nome_do_dispositivo`*. Por exemplo, para definir o endereço da interface eth0 como 192.168.12.154/30 com o broadcast padrão (opção `brd`), digite `ip addr add 192.168.12.154/30 brd + dev eth0`.

Para ter uma conexão ativa, você também precisa configurar o gateway padrão. Para definir um gateway para o sistema, digite `ip route add endereço_ip_do_gateway`. Para traduzir um endereço IP para outro, use `nat`: `ip route add nat endereço_ip via outro_endereço_ip`.

Para exibir todos os dispositivos, use `ip link ls`. Para exibir apenas as interfaces em execução, use `ip link ls up`. Para imprimir as estatísticas de interface de um dispositivo, digite `ip -s link ls nome_do_dispositivo`. Para ver os endereços dos dispositivos, digite `ip addr`. Na saída do comando `ip addr`, você também pode encontrar informações sobre os endereços MAC dos dispositivos. Para mostrar todas as rotas, use `ip route show`.

Para obter mais informações sobre como usar o `ip`, digite `ip help` ou consulte a página de manual de `ip(8)`. A opção `help` também está disponível para todos os subcomandos `ip`. Se, por exemplo, você precisar de ajuda para `ip addr`, digite `ip addr help`. Encontre o manual do `ip` em `/usr/share/doc/packages/iproute2/ip-cref.pdf`.

23.6.2.2 Testando uma conexão com o comando ping

O comando `ping` é a ferramenta padrão para testar o funcionamento de uma conexão TCP/IP. Ele usa o protocolo ICMP para enviar um pequeno pacote de dados, o datagrama ECHO_REQUEST, para o host de destino, solicitando uma resposta imediata. Se isso funcionar, o `ping` exibirá uma mensagem que indica que o link da rede está basicamente funcionando.

O `ping` vai além de simplesmente testar a função da conexão entre dois computadores; ele também fornece algumas informações básicas sobre a qualidade da conexão. No Exemplo 23.10, "Saída do comando ping" (p 356), você pode ver um exemplo da saída do `ping`. A penúltima linha contém informações sobre o número de pacotes transmitidos, o número de pacotes perdidos e o tempo total da execução do `ping`.

No destino, você pode usar o nome de host ou endereço IP, por exemplo, `ping example.com` ou `ping 192.168.3.100`. O programa enviará pacotes até que você pressione Ctrl + C.

Se você só precisar verificar a funcionalidade da conexão, poderá limitar o número dos pacotes com a opção `-c`. Por exemplo, para limitar o ping a três pacotes, digite `ping -c 3 exemplo.com`.

Exemplo 23.10 *Saída do comando ping*

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

O intervalo padrão entre dois pacotes é um segundo. Para mudar o intervalo, o ping fornece a opção `-i`. Por exemplo, para aumentar o intervalo do ping para dez segundos, digite `ping -i 10 exemplo.com`.

Em um sistema com vários dispositivos de rede, às vezes é útil enviar o ping através de um endereço de interface específico. Para isso, use a opção `-I` com o nome do dispositivo selecionado, por exemplo, `ping -I wlan1 exemplo.com`.

Para obter mais opções e informações sobre como usar o ping, digite `ping -h` ou consulte a página de manual de `ping (8)`.

DICA: Executando ping em endereços IPv6

Para endereços IPv6, use o comando `ping6`. Observe que, para executar ping em endereços locais de link, deve-se especificar a interface com `-I`. O comando a seguir funcionará se o endereço for acessível via `eth1`:

```
ping6 -I eth1 fe80::117:21ff:feda:a425
```

23.6.2.3 Configurando a rede com o ifconfig

`ifconfig` é uma ferramenta de configuração de rede.

NOTA: ifconfig e ip

A ferramenta `ifconfig` está obsoleta. Em vez disso, use `ip`. Ao contrário do `ip`, pode-se usar `ifconfig` apenas para configuração de interfaces. Ele limita nomes de interface a 9 caracteres.

Sem argumentos, o `ifconfig` exibe o status das interfaces atualmente ativas. Como você pode ver em Exemplo 23.11, "Saída do comando `ifconfig`" (p 357), o `ifconfig` tem uma saída detalhada e bem organizada. A saída também contém informações sobre o endereço MAC do seu dispositivo (o valor de `HWaddr`) na primeira linha.

Exemplo 23.11 *Saída do comando ifconfig*

```
eth0      Link encap:Ethernet  HWaddr 00:08:74:98:ED:51
          inet6 addr: fe80::208:74ff:fe98:ed51/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:634735 errors:0 dropped:0 overruns:4 frame:0
          TX packets:154779 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:162531992 (155.0 Mb)  TX bytes:49575995 (47.2 Mb)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:533234 (520.7 Kb)  TX bytes:533234 (520.7 Kb)

wlan1     Link encap:Ethernet  HWaddr 00:0E:2E:52:3B:1D
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:2eff:fe52:3b1d/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45978185 (43.8 Mb)  TX bytes:7526693 (7.1 MB)
```

Para obter mais opções e informações sobre como usar o `ifconfig`, digite `ifconfig -h` ou consulte a página de manual de `ifconfig (8)`.

23.6.2.4 Configurando o roteamento com route

`route` é um programa usado para manipular a tabela de roteamento IP. Você pode usá-lo para ver sua configuração de roteamento e adicionar ou remover rotas.

NOTA: route e ip

O programa `route` está obsoleto. Em vez disso, use `ip`.

`O comando route será especialmente útil se você precisar de informações rápidas e compreensíveis sobre a configuração do roteamento para identificar problemas de roteamento.` Para ver a configuração de roteamento atual, digite `route-n` as `root.`

Exemplo 23.12 *Saída do comando route -n*

```
route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.20.0.0       *               255.255.248.0   U         0 0          0 eth0
link-local      *               255.255.0.0     U         0 0          0 eth0
loopback        *               255.0.0.0       U         0 0          0 lo
default         styx.exam.com   0.0.0.0         UG        0 0          0 eth0
```

Para obter mais informações sobre como usar o route, digite `route -h` ou consulte a página de manual de `route (8)`.

23.6.3 Scripts de inicialização

Além dos arquivos de configuração descritos acima, há também vários scripts que carregam os programas de rede durante o boot da máquina. Eles são iniciados assim que o sistema é alternado para um dos *níveis de execução multiusuário*. Alguns desses scripts são descritos na Tabela 23.9, “Alguns scripts de inicialização para programas de rede” (p 359).

Tabela 23.9 Alguns scripts de inicialização para programas de rede

`/etc/init.d/network`	Este script controla a configuração das interfaces de rede. Se o serviço `network` não tiver sido iniciado, nenhuma interface de rede será implementada.
`/etc/init.d/xinetd`	Inicia o xinetd. O xinetd pode ser usado para disponibilizar os serviços do servidor no sistema. Por exemplo, ele pode iniciar o vsftpd sempre que uma conexão FTP for inicializada.
`/etc/init.d/rpcbind`	Inicia o utilitário rpcbind, que converte os números de programa RPC em endereços universais. Necessário para os serviços RPC, como um servidor NFS.
`/etc/init.d/nfsserver`	Inicia o servidor NFS.
`/etc/init.d/postfix`	Controla o processo de postfix.
`/etc/init.d/ypserv`	Inicia o servidor NIS.
`/etc/init.d/ypbind`	Inicia o cliente NIS.

23.7 Configurando dispositivos de ligação

Em alguns sistemas, existe a necessidade de implementar conexões de rede compatíveis com outros requisitos além dos padrões de disponibilidade ou segurança de dados de um dispositivo Ethernet comum. Nesses casos, vários dispositivos Ethernet podem ser agregados a um único dispositivo de ligação.

A configuração do dispositivo de ligação é feita através das opções dos módulos de ligação. O comportamento é afetado principalmente pelo modo do dispositivo de ligação. Por padrão, o modo é `mode=active-backup`, o que significa que um dispositivo escravo diferente será ativado se houver falha no escravo ativo.

DICA: Ligação e Xen

O uso de dispositivos de ligação só é interessante para máquinas que tenham várias placas de rede reais disponíveis. Na maioria das configurações, isso significa que você deve usar a configuração de ligação apenas no Domain0. Somente se você tiver várias placas de rede atribuídas a um sistema Convidado VM é que também poderá ser útil configurar a ligação em um Convidado VM.

Para configurar um dispositivo de ligação, siga este procedimento:

1 Execute *YaST* > *Dispositivos de Rede* > *Configurações de Rede*.

2 Use *Adicionar* e mude o *Tipo de Dispositivo* para *Ligação*. Continue com *Avançar*.

3 Escolha como vai atribuir o endereço IP ao dispositivo de ligação. Há três métodos à sua disposição:

- Nenhum Endereço IP

- Endereço Dinâmico (com DHCP ou Zeroconf)
- Endereço IP atribuído estaticamente

Use o método mais apropriado ao seu ambiente.

4. Na guia *Escravos Vinculados*, selecione os dispositivos Ethernet que devem ser incluídos na ligação ativando as caixas de seleção relacionadas.

5. Edite as *Opções do Driver de Vinculação*. Os seguintes modos estão disponíveis para configuração:

    - balance-rr
    - active-backup
    - balance-xor
    - broadcast
    - 802.3ad
    - balance-tlb
    - balance-alb

6. Verifique se o parâmetro `miimon=100` foi adicionado às *Opções do Driver de Vinculação*. Sem esse parâmetro, a integridade dos dados não é verificada regularmente.

7. Clique em *Avançar* e saia do YaST clicando em *OK* para criar o dispositivo.

Todos os modos, e muito mais opções, são explicados em detalhes no *Linux Ethernet Bonding Driver HOWTO* encontrado em `/usr/src/linux/Documentation/networking/bonding.txt` após a instalação do pacote `kernel-source`.

23.7.1 Hotplug de escravos associados

Em ambientes de rede específicos (como os de Alta Disponibilidade), há casos em que você precisa substituir uma interface de escravo associado por outra. O motivo pode

ser uma falha constante no dispositivo de rede. A solução é configurar o hotplug dos escravos associados.

A ligação é configurada como de costume (de acordo com `man 5 ifcfg-bonding`), por exemplo:

```
ifcfg-bond0
          STARTMODE='auto' # or 'onboot'
          BOOTPROTO='static'
          IPADDR='192.168.0.1/24'
          BONDING_MASTER='yes'
          BONDING_SLAVE_0='eth0'
          BONDING_SLAVE_1='eth1'
          BONDING_MODULE_OPTS='mode=active-backup miimon=100'
```

mas os escravos são especificados com `STARTMODE=hotplug` e `BOOTPROTO=none`:

```
ifcfg-eth0
          STARTMODE='hotplug'
          BOOTPROTO='none'

ifcfg-eth1
          STARTMODE='hotplug'
          BOOTPROTO='none'
```

`BOOTPROTO=none` usa as opções de ethtool (quando fornecidas), mas não define o link ativo no `ifup eth0`. O motivo é que a interface do escravo é controlada pelo master de ligação.

`STARTMODE=hotplug` faz com que a interface do escravo se una à ligação automaticamente assim que estiver disponível.

As regras do `udev` em `/etc/udev/rules.d/70-persistent-net.rules` devem ser mudadas para corresponder ao dispositivo pelo ID do barramento (udev `KERNELS` keyword equal to "SysFS BusID" as visible in `hwinfo --netcard`), e não pelo endereço MAC, para permitir a substituição do hardware com defeito (uma placa de rede no mesmo slot, mas com um MAC diferente) e evitar confusão conforme a ligação modifica o endereço MAC de todos os seus escravos.

Por exemplo:

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
KERNELS=="0000:00:19.0", ATTR{dev_id}=="0x0", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"
```

No momento do boot, `/etc/init.d/network` não espera o hotplug dos escravos, mas sim a ligação ficar pronta, o que requer no mínimo um escravo disponível. Quando uma das interfaces dos escravos é removida (desvincular do driver NIC, `rmmod` do driver NIC ou remoção do hotplug do PCI verdadeira) do sistema, o kernel a remove automaticamente da ligação. Quando uma nova placa é adicionada ao sistema (substituição do hardware no slot), o `udev` a renomeia usando a regra de nome persistente baseada em barramento com o nome do escravo e chama o `ifup` para ela. A chamada do `ifup` une-a automaticamente à ligação.

23.8 smpppd como Assistente de Discagem

Alguns usuários domésticos não possuem uma linha dedicada de conexão à Internet. Em vez disso, usam conexões por discagem. Dependendo da forma de discagem (ISDN ou DSL), a conexão é controlada por ipppd ou pppd. Basicamente, tudo o que precisa ser feito para estabelecer a conexão é iniciar esses programas corretamente.

Se você tiver uma conexão com tarifa fixa que não gere custos adicionais para a conexão por discagem, basta iniciar o respectivo daemon. Controle a conexão por discagem com um applet de área de trabalho ou uma interface de linha de comando. Se o portal de Internet não for o host que você estiver usando, você poderá controlar a conexão por discagem por intermédio de um host de rede.

É neste momento que o smpppd (SUSE Meta PPP Daemon) é envolvido. Ele oferece uma interface uniforme para programas auxiliares e funciona nas duas direções. Primeiro, ele programa o pppd ou ipppd necessário e controla suas propriedades de discagem. Em segundo lugar, disponibiliza diversos provedores aos programas do usuário e transmite informações sobre o atual status da conexão. Já que o smpppd também pode ser controlado por meio da rede, é adequado para controlar conexões por discagem à Internet de uma estação de trabalho de uma sub-rede privada.

23.8.1 Configurando o smpppd

As conexões fornecidas pelo smpppd são automaticamente configuradas pelo YaST. Os programas por discagem KInternet e cinternet efetivos também são pré-configurados.

Configurações manuais somente são necessárias para configurar recursos adicionais do smpppd, como o controle remoto.

O arquivo de configuração do smpppd é o `/etc/smpppd.conf`. Por padrão, ele não habilita o controle remoto. As opções mais importantes desse arquivo de configuração são:

open-inet-socket = *yes|no*
: Para controlar o smpppd pela rede, defina essa opção como `yes`. O smpppd escuta na porta `3185`. Se esse parâmetro for definido como `yes`, os parâmetros `bind-address`, `host-range` e `password` deverão ser definidos da mesma forma.

bind-address = *endereço ip*
: Se um host tiver diversos endereços IP, use esse parâmetro para determinar o endereço IP em que o smpppd deve aceitar conexões. O padrão é escutar em todos os endereços.

host-range = *ip mín.ip máx.*
: O parâmetro `host-range` define uma faixa de rede. Os hosts cujos endereços IP se situam dentro dessa faixa recebem acesso ao smpppd. O acesso é recusado a todos os hosts localizados fora dessa faixa.

password = *senha*
: Ao atribuir uma senha, limite os clientes a hosts autorizados. Como se trata de uma senha de texto simples, não é recomendável superestimar a segurança oferecida. Se nenhuma senha for atribuída, todos os clientes terão permissão para acessar o smpppd.

slp-register = *yes|no*
: Com esse parâmetro, o serviço smpppd pode ser anunciado na rede por meio do SLP.

Mais informações sobre o smpppd estão disponíveis nas páginas do manual `smpppd(8)` e `smpppd.conf(5)`.

23.8.2 Configurando o cinternet para uso remoto

É possível usar o cinternet para controlar um smpppd local ou remoto. cinternet é o equivalente de linha de comando ao KInternet gráfico. Para preparar esses utilitários para uso com um smpppd remoto, edite o arquivo de configuração `/etc/smpppd-c.conf` manualmente ou por meio do cinternet. Esse arquivo usa apenas quatro opções:

sites = *`lista de locais`*
: É a *`lista de locais`* onde os front ends procuram smpppd. Os front ends testam as opções na ordem especificada. A opção `local` solicita o estabelecimento de uma conexão com o smpppd local. A opção `gateway` aponta para um smpppd no gateway. O `config-file` indica que deve-se estabelecer a conexão com o smpppd especificado nas opções `server` e `port` em `/etc/smpppd-c.conf`. O `slp` ordena que os front ends se conectem com um smpppd encontrado por SLP.

server = *`servidor`*
: O host em que o smpppd é executado.

port = *`porta`*
: A porta em que o smpppd é executado.

password = *`senha`*
: Senha selecionada para o smpppd.

Se o smpppd estiver ativo, tente acessá-lo. Por exemplo, com `cinternet --verbose --interface-list`. Em caso de dificuldade nesse ponto, consulte as páginas de manual de `smpppd-c.conf(5)` e de `cinternet(8)`.

Serviços SLP na rede

24

O *SLP* foi criado para simplificar a configuração dos clientes em rede dentro de uma rede local. Para configurar um cliente em rede, inclusive todos os serviços necessários, o administrador normalmente precisa ter conhecimento detalhado dos servidores disponíveis na rede. O SLP divulga a disponibilidade de serviços selecionados a todos os clientes da rede local. Os aplicativos que dão suporte ao SLP podem usar as informações distribuídas e podem ser configurados automaticamente.

O SUSE® Linux Enterprise Desktop suporta a instalação com o uso de fontes de instalação fornecidas via SLP e contém diversos serviços de sistema com suporte integrado a SLP. O YaST e o Konqueror possuem front ends apropriados para SLP. Você pode usar o SLP para oferecer funções centrais aos clientes em rede, como servidor de instalação, servidor de arquivos ou servidor de impressão no sistema.

IMPORTANTE: Suporte a SLP no SUSE Linux Enterprise Desktop

Serviços que oferecem suporte ao SLP: cupsd, rsyncd, ypserv, openldap2, ksysguardd, saned, kdm, vnc, login, smpppd, rpasswd, postfix e sshd (via fish).

24.1 Instalação

Todos os pacotes necessários são instalados por padrão. No entanto, se você quiser fornecer serviços via SLP, verifique se o pacote `openslp-server` está instalado.

24.2 Ativando o SLP

O slpd deve ser executado no sistema para oferecer serviços pelo SLP. Se a máquina pode operar apenas como cliente a não oferece serviços, não é necessário ter slpd em execução nela. Assim como a maioria dos serviços de sistema no SUSE Linux Enterprise Desktop, o daemon slpd é controlado por um script `init` separado. Após a instalação, o daemon fica inativo por padrão. Para ativá-lo temporariamente, execute `rcslpd start` enquanto usuário `root` ou `rcslpd stop` para pará-lo. Efetue uma verificação de reinicialização ou status com `restart` ou `status`. Se for necessário que o slpd fique sempre ativo após a inicialização, habilite o slpd no YaST *Sistema* > *Serviços do Sistema (Nível de Execução)* ou execute o comando `insserv slpd` como `root`.

24.3 Front ends SLP no SUSE Linux Enterprise Desktop

Para localizar os serviços fornecidos por SLP em sua rede, use um front end SLP como `slptool` (pacote `openslp`) ou o YaST:

slptool
: slptool é um programa de linha de comando capaz de anunciar perguntas SLP na rede ou serviços proprietários. `slptool --help` lista todas as opções e funções disponíveis. Por exemplo, para encontrar todos os servidores de horário que se anunciam na rede atual, execute o comando:

```
slptool findsrvs service:ntp
```

YaST
: O YaST também oferece um browser SLP. Porém, esse browser não está disponível no Centro de Controle do YaST. Para iniciá-lo, execute `yast2 slp` como usuário `root`. Clique em um *Tipo de Serviço* na lateral esquerda para ver mais informações sobre o serviço.

24.4 Fornecendo serviços por SLP

Muitos aplicativos no SUSE Linux Enterprise Desktop já têm suporte integrado ao SLP com o uso da biblioteca `libslp`. Se um serviço não tiver sido compilado com o suporte ao SLP, use um dos métodos a seguir para disponibilizá-lo por SLP:

Registro estático com `/etc/slp.reg.d`

Crie um arquivo de registro separado para cada novo serviço. Este é um exemplo de registro do serviço de scanner:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

A linha mais importante desse arquivo é a linha *URL do serviço*, que começa com `service:`. Essa linha contém o tipo de serviço (`scanner.sane`) e o endereço em que o serviço está disponível no servidor. *`$HOSTNAME`* é automaticamente substituída pelo nome completo do host. Em seguida, vem o nome da porta TCP em que o serviço em questão pode ser encontrado, separado por dois-pontos. A seguir, especifique o idioma em que o serviço deve ser exibido e a duração do registro em segundos. Esses dados devem ser separados do URL do serviço por vírgulas. Defina o valor da duração do registro entre `0` e `65535. O valor` 0 impede o registro. `O valor` 65535 elimina todas as restrições.

O arquivo de registro também contém as duas variáveis `watch-port-tcp` e `description`. `watch-port-tcp` vincula o anúncio do serviço SLP à atividade do serviço em questão fazendo com que o slpd verifique o status do serviço. A segunda variável contém uma descrição mais precisa do serviço que é exibido nos browsers apropriados.

Registro estático com `/etc/slp.reg`

A única diferença entre esse método e o procedimento de `/etc/slp.reg.d` é que todos os serviços são agrupados em um arquivo central.

Registro dinâmico com `slptool`

Se um serviço precisar ser registrado dinamicamente sem a necessidade de arquivos de configuração, use o utilitário de linha de comando slptool. O mesmo utilitário

também pode ser usado para cancelar o registro de uma oferta de serviço existente sem reiniciar o slpd.

24.5 Para obter mais informações

RFC 2608, 2609, 2610
: O RFC 2608 geralmente trata da definição de SLP. O RFC 2609 trata da sintaxe dos URLs de serviço usados em maior detalhe e o RFC 2610 trata do DHCP via SLP.

`http://www.openslp.org`
: A home page do projeto OpenSLP.

`/usr/share/doc/packages/openslp`
: Este diretório apresenta a documentação do SLP que acompanha o pacote `openslp-server`, incluindo o `README.SuSE` com detalhes do SUSE Linux Enterprise Desktop, os RFCs e dois documentos HTML de introdução. Os programadores que desejarem usar as funções do SLP podem obter mais informações no *Programmers Guide* (Guia do programador), incluído no pacote `openslp-devel`.

Sincronização de horário com NTP

25

O mecanismo NTP (network time protocol) é um protocolo para sincronizar o horário do sistema na rede. Primeiro, uma máquina pode obter o horário de um servidor, que é uma fonte de horário confiável. Segundo, a máquina pode agir como uma fonte de horário para outros computadores na rede. O objetivo é duplo: manter o tempo absoluto e a sincronização do horário do sistema de todas as máquinas na rede.

Manter um horário exato do sistema é importante em várias situações. Geralmente, o relógio do hardware incorporado não atende aos requisitos dos aplicativos, como bancos de dados ou clusters. A correção manual do horário do sistema levaria a problemas severos pois, por exemplo, um pulo inverso pode causar o mau funcionamento de aplicativos críticos. Em uma rede, geralmente é necessário sincronizar o horário do sistema de todas as máquinas, porém, o ajuste manual do horário não é um bom método. O NTP dispõe de um mecanismo para resolver esses problemas. O serviço NTP ajusta continuamente o horário do sistema com a ajuda de servidores de horário confiáveis na rede. Ele habilita também o gerenciamento de relógios de referência local como relógios controlados pelo rádio.

NOTA

Para habilitar a sincronização de horário por meio do diretório ativo, siga as instruções no Procedure “Joining an AD Domain” (↑*Security Guide*).

25.1 Configurando um cliente NTP com YaST

O daemon do NTP (`ntpd`) que acompanha o pacote `ntp` vem predefinido para usar o relógio do computador como a referência de horário. Entretanto, o uso do relógio do hardware só serve como fallback nos casos em que não há uma fonte de horário mais precisa disponível. O YaST facilita a configuração de um cliente NTP.

25.1.1 Configuração Básica

A configuração do cliente NTP do YaST (*Serviços de Rede* > *Configuração NTP*) é composta por guias. Defina o modo de iniciar do `ntpd` e o servidor para consulta na guia *Configurações Gerais*.

Apenas Manualmente
: Selecione *Apenas Manualmente* para iniciar manualmente o daemon `ntpd`.

Agora e ao Inicializar
: Selecione *Agora e ao Inicializar* para iniciar o `ntpd` automaticamente quando o sistema for inicializado. Essa configuração é altamente recomendada. Em seguida, configure o servidor conforme descrito na Seção 25.1.2, “Mudando a configuração básica” (p 372).

25.1.2 Mudando a configuração básica

Os servidores e outras fontes de horário para a consulta do cliente estão listados na guia *Configurações Gerais*. Modifique esta lista conforme necessário com *Adicionar*, *Editar* e *Apagar*. *Exibir Registro* fornece a possibilidade de exibir os arquivos de registro do seu cliente.

Clique em *Adicionar* para adicionar uma nova fonte de informação de horário. Na caixa de diálogo seguinte, selecione o tipo de fonte com a qual a sincronização de horário deve ser realizada. As seguintes opções estão disponíveis:

Figura 25.1 *YaST: servidor NTP*

Servidor

Na lista suspensa *Selecionar* (veja a Figura 25.1, "YaST: servidor NTP" (p 373)), determine se é para configurar a sincronização de horário usando um servidor de horário da rede local (*Servidor NTP Local*) ou um servidor de horário baseado na Internet que controla o seu fuso horário (*Servidor NTP Público*). Para um servidor de horário local, clique em *Busca* para iniciar uma consulta SLP por servidores de horário disponíveis na sua rede. Selecione o servidor de horário mais adequado a partir da lista de resultados de pesquisa e saia da caixa de diálogo com *OK*. Para um servidor de horário público, selecione o país (fuso horário) e um servidor adequado da lista sob *Servidor NTP Público*, em seguida, saia da caixa de diálogo com *OK*. Na caixa de diálogo principal, teste a disponibilidade do servidor selecionado com *Testar*. *Opções* permite que você especifique opções adicionais para o `ntpd`.

Com o uso de *Opções de Controle de Acesso*, você pode restringir as ações que o computador remoto pode desempenhar com o daemon em execução no seu computador. Esse campo apenas será habilitado após marcar *Restringir Serviço NTP Apenas aos Servidores Configurados* na guia *Configurações de Segurança* (veja a Figura 25.2, "Configuração NTP Avançada: Configurações de Segurança" (p 375)). As opções correspondem às cláusulas `restrict` em `/etc/ntp.conf`. Por exemplo, `nomodify notrap noquery` não permite que o

servidor modifique as configurações de NTP do seu computador e use o recurso de detecção (um recurso de registro de eventos remotos) do seu daemon NTP. O uso dessas restrições é recomendado para os servidores fora de controle (por exemplo, na Internet).

Consulte `/usr/share/doc/packages/ntp-doc` (parte do pacote `ntp-doc`) para obter informações detalhadas.

Peer
: Um peer é uma máquina com a qual é estabelecido um relacionamento simétrico: ele atua como servidor de horário e como cliente. Para usar um peer na mesma rede em vez de um servidor, digite o endereço do sistema. O restante da caixa de diálogo é igual à caixa de diálogo *Servidor*.

Relógio controlado pelo rádio
: Para usar um relógio controlado pelo rádio no seu sistema para a sincronização de horário, insira o tipo de relógio, o número da unidade, o nome do dispositivo e outras opções nesta caixa de diálogo. Clique em *Calibração do Driver* para ajustar o driver. Informações detalhadas sobre a operação de um rádio relógio local estão disponíveis em `/usr/share/doc/packages/ntp-doc/html/refclock.htm`.

Transmissão de saída
: Consultas e informações sobre horário também podem ser transmitidas na rede. Nesta caixa de diálogo, insira o endereço ao qual estas transmissões devem ser enviadas. Não ative a transmissão a menos que você tenha uma fonte de horário confiável como um relógio controlado por rádio.

Transmissão de entrada
: Se você deseja que o seu cliente receba suas informações através de transmissão, insira o endereço do qual os respectivos pacotes devem ser aceitos nestes campos.

***Figura 25.2** Configuração NTP Avançada: Configurações de Segurança*

Na guia *Configurações de Segurança* (veja a Figura 25.2, “Configuração NTP Avançada: Configurações de Segurança” (p 375)), determine se o `ntpd` deve ser iniciado em um chroot jail. Por padrão, a opção *Executar Daemon NTP em Chroot Jail* está ativada. Isso aumenta a segurança em caso de ataque ao `ntpd`, já que impede o invasor de comprometer todo o sistema.

Restringir Serviço NTP Apenas aos Servidores Configurados aumenta a segurança do seu sistema ao não permitir que os computadores remotos vejam e modifiquem as configurações de NTP do seu computador e que usem o recurso de detecção para o registro de eventos remotos. Uma vez habilitadas, essas restrições se aplicam a todos os computadores remotos, a menos que você anule as opções de controle de acesso para computadores individuais na lista de fontes de horário na guia *Configurações Gerais*. Para todos os outros computadores remotos, só é permitida a consulta de horário local.

Habilite *Abrir Porta no Firewall* se o SuSEfirewall2 estiver ativo (ele fica ativo por padrão). Se você manter a porta fechada, não será possível estabelecer uma conexão com o servidor de horário.

25.2 Configurando manualmente o NTP na rede

A forma mais fácil de usar um servidor de horário na rede é definir parâmetros de servidor. Por exemplo, se um servidor de horário denominado `ntp.exemplo.com` estiver acessível na rede, adicione seu nome ao arquivo `/etc/ntp.conf` incluindo a seguinte linha:

```
server ntp.example.com
```

Para adicionar mais servidores de horário, insira linhas adicionais com a palavra-chave `server`. Após inicializar o `ntpd` com o comando `rcntp start`, leva cerca de uma hora para estabilizar o horário e criar o arquivo drift que corrige o relógio do computador local. Com o arquivo de descompasso, o erro sistemático do relógio do hardware pode ser computado assim que o computador for ligado. A correção é usada imediatamente, resultando em uma estabilidade maior do horário do sistema.

Há duas maneiras possíveis de usar o mecanismo NTP como cliente: primeiro, o cliente pode consultar o horário a partir de um servidor conhecido em intervalos regulares. Com vários clientes, esta abordagem pode causar uma carga alta no servidor. Segundo, o cliente pode esperar por transmissões de NTP enviadas por servidores de horário de transmissão na rede. Esta abordagem tem a desvantagem de que a qualidade do servidor é desconhecida e um servidor transmitindo a informação errada pode causar problemas graves.

Se o horário for obtido através de uma transmissão, você não precisará do nome do servidor. Neste caso, insira a linha `broadcastclient` no arquivo de configuração `/etc/ntp.conf`. Para usar um ou mais servidores de horário conhecidos exclusivamente, insira seus nomes na linha iniciando com `servers`.

25.3 Sincronização de horário dinâmica em tempo de execução

Se o sistema for inicializado sem conexão de rede, o `ntpd` será iniciado, mas não conseguirá resolver os nomes DNS dos servidores de horário definidos no arquivo de

configuração. Isso pode ocorrer se você usar o Gerenciador de Rede com uma WLAN criptografada.

Para que o `ntpd` resolva os nomes DNS em tempo de execução, defina a opção `dynamic`. Em seguida, quando a rede é estabelecida algum tempo após a inicialização, o `ntpd` procura os nomes novamente e acessa os servidores de horário para capturar a hora.

Edite manualmente o `/etc/ntp.conf` e adicione `dynamic` a uma ou mais entradas `server`:

```
server ntp.example.com dynamic
```

Se preferir, use o YaST e faça o seguinte:

1. No YaST, clique em *Serviços de Rede* > *Configuração NTP*.

2. Selecione o servidor que deseja configurar. Em seguida, clique em *Editar*.

3. Ative o campo *Opções* e adicione `dynamic`. Separe-o por um espaço, se já houver outras opções digitadas.

4. Clique em *OK* para fechar a caixa de diálogo de edição. Repita a etapa anterior para mudar todos os servidores conforme desejado.

5. Por fim, clique em *OK* para gravar as configurações.

25.4 Configurando um relógio de referência local

O pacote de software `ntpd` inclui drivers para conexão de relógios locais de referência. Uma lista de relógios suportados está disponível no pacote `ntp-doc` no arquivo `/usr/share/doc/packages/ntp-doc/html/refclock.htm`. Cada driver está associado a um número. No NTP, a configuração real é feita por pseudos endereços IP. Os relógios são inseridos no arquivo `/etc/ntp.conf` como se existissem na rede. Para este propósito, endereços IP especiais são atribuídos a eles no formato `127.127.`*`t`*`.`*`u`*. Aqui, *`t`* representa o tipo de relógio e determina o driver a ser usado e *`u`* representa a unidade, que determina a interface usada.

Normalmente, os drivers individuais têm parâmetros especiais que descrevem detalhes de configuração. O arquivo /usr/share/doc/packages/ntp-doc/drivers/driver*NN*.html (onde *NN* é o número do driver) fornece informações sobre o tipo específico de relógio. Por exemplo, o relógio "type 8" (relógio controlado por rádio na interface serial) exige um modo adicional que especifica o relógio de forma mais precisa. O módulo de recebimento Conrad DCF77, por exemplo, tem o modo 5. Para usar este relógio como referência preferida, especifique a palavra-chave prefer. A linha do servidor completa para um módulo de recebimento Conrad DCF77 seria:

```
server 127.127.8.0 mode 5 prefer
```

Outros relógios seguem o mesmo padrão. Após a instalação do pacote ntp-doc, a documentação do NTP fica disponível no diretório /usr/share/doc/packages/ntp-doc. O arquivo /usr/share/doc/packages/ntp-doc/refclock.html fornece links para as páginas que descrevem os parâmetros do driver.

Usando o NetworkManager 26

O NetworkManager é a solução ideal para laptops e outros computadores portáteis. Ele suporta tipos e padrões de criptografia avançados para conexões de rede, incluindo conexões com rede protegidas por 802.1X. 802.1X é o "Padrão IEEE para Redes Locais e de Área Metropolitana — Controle de Acesso a Rede Baseado na Porta". Com o NetworkManager, você não precisa se preocupar em configurar interfaces de rede nem em alternar entre redes wireless ou com fio quando estiver em trânsito. O NetworkManager pode conectar-se automaticamente a redes wireless conhecidas ou gerenciar várias conexões de rede paralelamente, caso em que a conexão mais rápida é usada como padrão. Além disso, você pode alternar manualmente entre as redes disponíveis e gerenciar sua conexão de rede usando um applet na bandeja do sistema.

Várias conexões podem estar ativas simultaneamente, em vez de apenas uma. Isso lhe permite desplugar o laptop de uma Ethernet e permanecer conectado por uma conexão wireless.

26.1 Casos de uso para o NetworkManager

O NetworkManager dispõe de uma interface do usuário sofisticada e intuitiva, que permite aos usuários alternar facilmente seu ambiente de rede. Contudo, o NetworkManager não é uma solução adequada nos seguintes casos:

- O computador fornece serviços de rede para outros computadores de sua rede, por exemplo, se ele for um servidor DHCP ou DNS.

- Seu computador é um servidor Xen ou seu sistema é um sistema virtual dentro do Xen.

26.2 Habilitando ou desabilitando o NetworkManager

Em laptops, o NetworkManager está habilitado por padrão. No entanto, ele pode ser habilitado ou desabilitado a qualquer momento no módulo Configurações de Rede do YaST.

1 Execute o YaST e vá para *Dispositivos de Rede* > *Configurações de Rede*.

2 A caixa de diálogo *Configurações de Rede* é aberta. Vá até a guia *Opções Globais*.

3 Para configurar e gerenciar suas conexões de rede com o NetworkManager:

3a No campo *Método de Configuração da Rede*, selecione *Controlado por Usuário com o NetworkManager*.

3b Clique em *OK* e feche o YaST.

3c Configure as conexões de rede com o NetworkManager, conforme descrito na Seção 26.3, “Configurando conexões de rede” (p 381).

4 Para desativar o NetworkManager e controlar a rede da maneira comum:

4a No campo *Método de Configuração da Rede*, escolha *Método Tradicional com ifup*.

4b Clique em *OK*.

4c Configure a placa de rede com o YaST usando a configuração automática através do DHCP ou de um endereço IP estático. Se preferir, configure o modem com o YaST:

- Para conexões discadas, use *Dispositivos de Rede* > *Modem*.

- Para configurar um modem interno ou USB RDSI (ISDN), selecione *Dispositivos de Rede* > *ISDN*.

- Para configurar um modem USB DSL, selecione *Dispositivos de Rede* > *DSL*.

Há uma descrição detalhada da configuração de rede com o YaST disponível na Seção 23.4, "Configurando uma conexão de rede com o YaST" (p 318) e no Capítulo 20, *Rede local sem fio* (p 257).

26.3 Configurando conexões de rede

Após habilitar o NetworkManager no YaST, configure as conexões de rede com os front ends do NetworkManager disponíveis no KDE e no GNOME. As caixas de diálogo de configuração de rede para ambos os front ends são bem semelhantes. Elas apresentam guias para todos os tipos de conexões de rede, por exemplo, com fio, wireless, banda larga móvel, DSL e VPN. Em cada guia, você pode adicionar, editar ou apagar conexões do tipo em questão. Na caixa de diálogo de configuração do KDE, as guias apropriadas somente estarão ativas se o tipo de conexão estiver disponível no seu sistema (dependendo do hardware e do software). Por padrão, o KNetworkManager também exibe dicas de ferramentas abrangentes para os campos de entrada e as opções disponíveis em cada guia.

NOTA: Conexões Bluetooth

Atualmente, as conexões Bluetooth não podem ser configuradas com o NetworkManager.

Para abrir a caixa de diálogo de configuração da rede no GNOME, abra o menu principal e clique na entrada *Rede* à direita. Se preferir, pressione Alt + F2 e digite `nm-connection-editor` ou selecione *Sistema* > *Conexões de Rede* no Centro de Controle do GNOME.

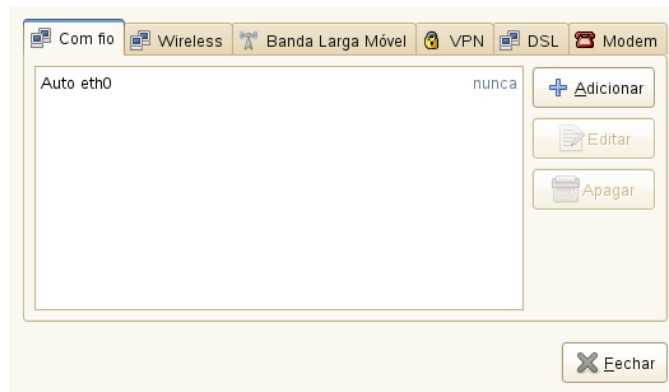
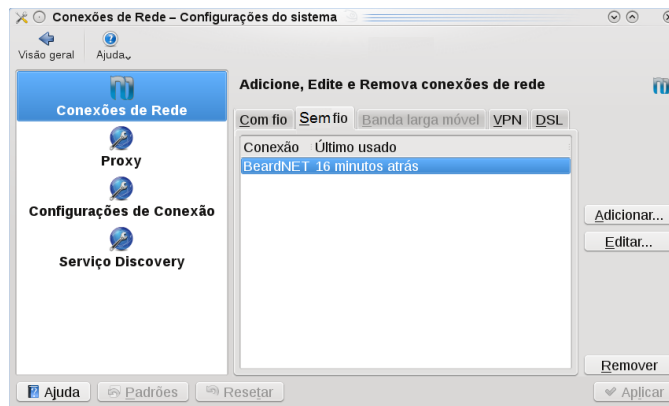
Figura 26.1 *Caixa de diálogo Conexões de Rede do GNOME*

Se você usa o KDE, abra o menu principal e clique em *Configurar a Área de Trabalho*. Em *Configurações Pessoais*, selecione *Configurações de Rede* (na guia *Geral*) para abrir a caixa de diálogo de configurações de rede.

Figura 26.2 *Caixa de diálogo de configuração de rede do KDE*

Se preferir, você também poderá iniciar as caixas de diálogo de configuração pelo applet NetworkManager na bandeja do sistema. No KDE, clique o botão esquerdo do mouse no ícone e selecione *Gerenciar Conexões*. No GNOME, clique o botão direito do mouse no ícone e selecione *Editar Conexões*.

NOTA: disponibilidade das opções

Dependendo da configuração do seu sistema, pode ser que você não tenha permissão para configurar conexões. Em um ambiente protegido, talvez algumas opções sejam bloqueadas ou exijam permissão de `root`. Consulte o administrador do sistema para obter os detalhes.

Procedimento 26.1 *Adicionando ou editando conexões*

Ao configurar conexões de rede com o NetworkManager, você também pode definir `conexões de sistema` que podem ser compartilhadas por todos os usuários. Diferentemente das `conexões de usuário`, as conexões de sistema são disponibilizadas logo após o NetworkManager ser iniciado, antes que qualquer usuário efetue login. Para obter mais detalhes sobre ambos os tipos de conexões, consulte a Seção 26.7.1, “Conexões de usuário e sistema” (p 393).

No momento, a opção de `conexão de sistema` não está disponível no KDE. Nesse caso, você precisa usar o YaST para configurar as conexões do sistema.

NOTA: redes ocultas

Para conectar a uma rede “oculta” (uma rede que não transmita seu serviço), você precisa saber o SSID (Service Set Identifier) ou o ESSID (Extended Service Set Identifier) da rede. Não é possível detectar automaticamente redes ocultas.

1 Na caixa de diálogo de configurações de rede, clique na guia referente ao tipo de conexão que deseja usar.

2 Clique em *Adicionar* para criar uma nova conexão ou selecione uma existente e clique em *Editar*.

3 Digite um *Nome da Conexão* e os respectivos detalhes da conexão.

4 No caso de uma rede oculta, digite o ESSID e os parâmetros de criptografia.

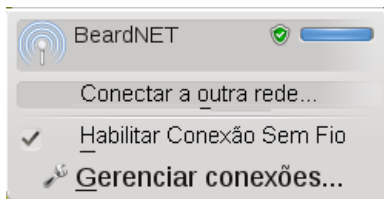
5 Você pode vincular a conexão a um determinado dispositivo, caso haja mais de um dispositivo físico disponível por tipo de conexão (por exemplo, quando a máquina está equipada com duas placas ethernet ou duas placas wireless).

Ao usar o KDE, faça isso usando a opção *Restringir à Interface*. Ao usar o GNOME, digite o *endereço MAC* do dispositivo ao qual deseja vincular a conexão e confirme as configurações.

6 Para que o NetworkManager use automaticamente determinada conexão, ative a seguinte opção para essa conexão: *Conectar Automaticamente* (KDE) ou *Stay connected when possible* (Permanecer conectado quando possível, no GNOME).

7 Para transformar uma conexão em `conexão de sistema`, ative *Disponível para todos os usuários* (GNOME). A criação e a edição de conexões de sistema exigem permissão de `root`.

Depois de confirmadas as mudanças, a conexão de rede recém-configurada será exibida na lista de redes disponíveis que aparece ao clicar no applet NetworkManager.

Figura 26.3 *KNetworkManager: conexões configuradas e disponíveis*

26.4 Usando o KNetworkManager

O front end KDE para NetworkManager é o applet KNetworkManager. Se a rede tiver sido configurada para controle do NetworkManager, em geral, o applet será iniciado automaticamente com o ambiente de área de trabalho e mostrado como um ícone na bandeja do sistema.

Se a bandeja do sistema não mostrar nenhum ícone de conexão de rede, provavelmente o applet não foi iniciado. Pressione Alt + F2 e digite `knetworkmanager` para iniciá-lo manualmente.

O KNetworkManager mostra apenas as redes wireless para as quais você configurou uma conexão. Ele oculta as conexões quando você está fora do âmbito de uma rede wireless ou quando o cabo da rede está desconectado, de forma a apresentar-lhe sempre as conexões que podem ser usadas.

26.4.1 Gerenciando conexões de rede com fio

Se o seu computador estiver conectado a uma rede por um cabo de rede, use o KNetworkManager para escolher a conexão de rede.

1 Clique o botão esquerdo do mouse no ícone do applet para mostrar um menu com as redes disponíveis. A conexão em uso no momento é selecionada no menu e marcada como *Ativa*.

2 Se desejar usar uma configuração diferente na rede com fio, clique em *Gerenciar Conexões* e adicione outra conexão com fio conforme descrito no Procedimento 26.1, "Adicionando ou editando conexões" (p 383).

3 Clique no ícone do KNetworkManager e selecione a conexão recém-configurada para ativá-la.

26.4.2 Gerenciando conexões de rede wireless

Por padrão, o KNetworkManager mostra apenas as redes wireless para as quais você configurou uma conexão, desde que estejam disponíveis e visíveis. Para conectar-se a um rede wireless pela primeira vez, faça o seguinte:

Procedimento 26.2 *Conectando a uma rede wireless*

1 Clique o botão esquerdo do mouse no ícone do applet e selecione *Criar Conexão de Rede*. O KNetworkManager mostra uma lista de redes wireless disponíveis visíveis, incluindo detalhes sobre força e segurança do sinal.

2 Para conectar-se a uma rede visível, selecione-a na lista e clique em *Conectar*. Se a rede estiver criptografada, uma caixa de diálogo será aberta. Escolha o tipo de *Segurança* que a rede usa e digite as credenciais apropriadas.

3 Para conectar-se a uma rede que não transmite seu identificador SSID ou ESSID e, portanto, não pode ser detectada automaticamente, selecione *Connect to Other Network with WLAN interface* (Conectar à Outra Rede com interface WLAN).

4 Na caixa de diálogo aberta, digite o SSID ou o ESSID e defina os parâmetros de criptografia, se necessário.

5 Confirme as mudanças e clique em *OK*. O NetworkManager ativa a nova conexão.

6 Para terminar uma conexão e desabilitar a rede wireless, clique no ícone do applet e desmarque *Habilitar Conexão Sem Fio*. Isso poderá ser útil quando você estiver no avião ou em outro ambiente que não autorize rede wireless.

Uma rede wireless escolhida explicitamente permanecerá conectada o máximo de tempo possível. Se um cabo de rede estiver acoplado durante esse tempo, quaisquer conexões definidas com *Conectar Automaticamente* serão conectadas enquanto a conexão wireless permanecer ativa.

26.4.3 Configurando sua placa wireless como um ponto de acesso

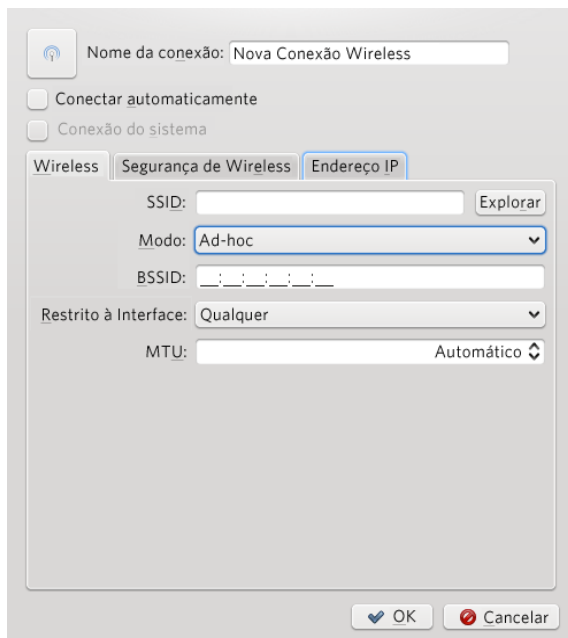
Se a placa wireless oferecer suporte ao modo de ponto de acesso, você poderá usar o NetworkManager para configuração.

NOTA: disponibilidade das opções

Dependendo da configuração de seu sistema, talvez não seja permitido configurar conexões. Em um ambiente protegido, talvez algumas opções sejam bloqueadas ou exijam permissão de `root`. Consulte o administrador do sistema para obter os detalhes.

---

1 Clique no applet do KNetworkManager e selecione *Criar Conexão de Rede* > *Nova Rede Ad-hoc*.

2 Na caixa de diálogo de configuração seguinte, digite um nome para a sua rede no campo *SSID*.

3 Defina a criptografia na guia *Segurança da Rede sem Fio*.

IMPORTANTE: redes wireless desprotegidas representam um risco de segurança

Se definir *Segurança* como `Nenhuma`, qualquer pessoa poderá se conectar à sua rede, reutilizar sua conectividade e interceptar sua conexão de rede. Use criptografia para restringir o acesso ao seu ponto de acesso e proteger sua conexão. Você pode escolher entre várias criptografias baseadas em WEP e WPA. Se não tiver certeza sobre qual tecnologia é mais apropriada para você, leia a Seção 20.3, “Autenticação” (p 259).

---

4 Na guia *Endereço IP*, verifique se a opção *Configurar* está definida como *Compartilhado* (opção padrão para redes ad-hoc).

5 Confirme sua configuração com *OK*.

26.4.4 Personalizando o KNetworkManager

Você pode personalizar alguns aspectos do KNetworkManager: o número de ícones exibidos na bandeja do sistema, as dicas de ferramentas que são mostradas e como armazenar sua senha e suas credenciais referentes às conexões de rede. Para obter mais informações sobre o último aspecto, consulte a Seção 26.7.2, “Armazenando senhas e credenciais” (p 394).

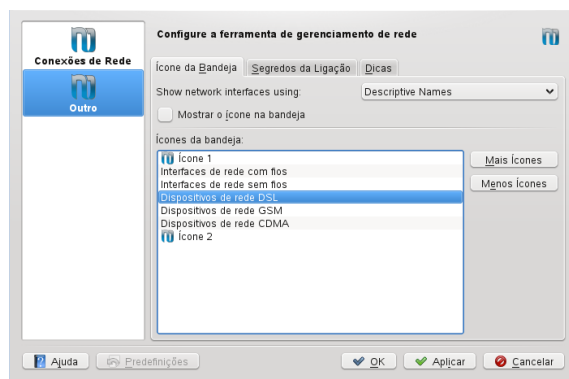
Para explorar as opções disponíveis, clique o botão direito do mouse no ícone do NetworkManager na bandeja do sistema, selecione *Gerenciar Conexões* e clique em *Outros* na lateral esquerda da caixa de diálogo de configurações.

***Procedimento 26.3** Configurando vários ícones da bandeja para o KNetworkManager*

Como o KNetworkManager pode manter várias conexões ativas ao mesmo tempo, você pode receber informações sobre o status de várias conexões em um relance. Para fazer isso, use vários ícones do NetworkManager na sua bandeja do sistema, cada um deles representando um grupo diferente de tipos de conexão (por exemplo, um ícone para conexões com fio, outro ícone para conexões wireless).

1. Na caixa de diálogo de configuração, alterne para a guia *Ícone da Bandeja*.

2. Clique em *Mais Ícones*. Uma nova entrada de ícone é exibida na lista.

3. Selecione os tipos de conexão de rede que serão representados por esse ícone e agrupe-os sob ele.

4 Confirme as mudanças.

Agora, a bandeja do sistema mostra vários ícones do NetworkManager, pelos quais você pode acessar os tipos de conexão vinculados a cada um.

Ao configurar uma conexão de rede conforme descrito em Procedimento 26.1, "Adicionando ou editando conexões" (p 383), o KNetworkManager também permite personalizar o ícone exibido para essa conexão. Para mudar o ícone, clique no botão do ícone ao lado de *Nome da Conexão* e, na caixa de diálogo a seguir, selecione o ícone da sua escolha. Após confirmadas as mudanças, o novo ícone é exibido na lista de conexões disponíveis que aparece quando se clica no ícone do KNetworkManager na bandeja do sistema.

26.5 Usando o applet NetworkManager do GNOME

No GNOME, é possível controlar o NetworkManager com o applet NetworkManager do GNOME. Se a rede estiver configurada para controle do NetworkManager, em geral, o applet será iniciado automaticamente com o ambiente de área de trabalho e exibido como ícone na bandeja do sistema.

Se a bandeja do sistema não mostrar nenhum ícone de conexão de rede, provavelmente o applet não foi iniciado. Pressione Alt + F2 e digite `nm-applet` para iniciá-lo manualmente.

26.5.1 Gerenciando conexões de rede com fio

Se o seu computador estiver conectado a uma rede existente com um cabo de rede, use o applet NetworkManager para escolher a conexão de rede.

1 Clique o botão esquerdo do mouse no ícone do applet para mostrar um menu com as redes disponíveis. A conexão usada no momento está selecionada no menu.

2 Para alternar para outra rede, escolha-a na lista.

3. Para desativar todas as conexões de rede, wireless ou não, clique o botão direito no ícone do applet e desmarque *Habilitar Rede*.

26.5.2 Gerenciando conexões de rede wireless

As redes wireless visíveis que estiverem disponíveis estarão listadas no menu do applet NetworkManager do GNOME em *Redes sem Fio*. A força do sinal de cada rede também é mostrada no menu. Redes wireless criptografadas são marcadas com um ícone de escudo.

Procedimento 26.4 *Conectando a uma rede wireless*

1. Para conectar-se a uma rede wireless, clique no ícone do applet e escolha uma entrada na lista de redes wireless disponíveis.

2. Se a rede estiver criptografada, uma caixa de diálogo será aberta. Ela mostra o tipo de criptografia usada pela rede (*Segurança da Rede sem Fio*) e contém uma série de campos de entrada de acordo com as respectivas configurações de criptografia e autenticação. Digite as credenciais apropriadas.

3. Para conectar-se a uma rede que não transmite seu identificador SSID ou ESSID e, portanto, não pode ser detectada automaticamente, clique no ícone do NetworkManager e escolha *Conectar à Rede Wireless Oculta*.

4. Na caixa de diálogo aberta, digite o SSID ou o ESSID em *Nome de Rede* e defina os parâmetros de criptografia, se necessário.

5. Para desabilitar a rede wireless, clique o botão direito do mouse no ícone do applet e desmarque *Habilitar Conexão sem Fio*. Isso poderá ser útil quando você estiver no avião ou em outro ambiente que não autorize rede wireless.

Uma rede wireless escolhida explicitamente permanecerá conectada o máximo de tempo possível. Se houver um cabo de rede conectado durante esse período, todas as conexões definidas como *Stay connected when possible* (Permanecer conectado quando possível) ficarão conectadas enquanto a conexão wireless continuar ativa.

26.5.3 Configurando sua placa wireless como um ponto de acesso

Se a placa wireless oferecer suporte ao modo de ponto de acesso, você poderá usar o NetworkManager para configuração.

NOTA: disponibilidade das opções

Dependendo da configuração de seu sistema, talvez não seja permitido configurar conexões. Em um ambiente protegido, talvez algumas opções sejam bloqueadas ou exijam permissão de `root`. Consulte o administrador do sistema para obter os detalhes.

---

1 Clique no applet NetworkManager e selecione *Criar Nova Rede sem Fio*.

2 Digite um *Nome da Rede* e defina a criptografia a ser usada com a lista suspensa *Segurança da Rede sem Fio*.

IMPORTANTE: redes wireless desprotegidas representam um risco de segurança

Se você definir *Segurança da Rede sem Fio* como `Nenhuma`, qualquer pessoa poderá se conectar à sua rede, reutilizar sua conectividade e interceptar sua conexão de rede. Use criptografia para restringir o acesso ao seu ponto de acesso e proteger sua conexão. Você pode escolher entre várias criptografias baseadas em WEP e WPA. Se não tiver certeza sobre qual tecnologia é mais apropriada para você, leia a Seção 20.3, “Autenticação” (p 259).

26.6 NetworkManager e VPN

O NetworkManager suporta várias tecnologias de VPN (Virtual Private Network). Para cada tecnologia, o SUSE Linux Enterprise Desktop possui um pacote básico com suporte genérico ao NetworkManager. Além disso, você também precisa instalar o respectivo pacote específico da área de trabalho para o seu applet.

NovellVPN
: Para usar esta tecnologia VPN, instale

    - `NetworkManager-novellvpn` e
    - `NetworkManager-novellvpn-kde4` ou `NetworkManager-novellvpn-gnome`.

    No momento, o suporte do NovellVPN ao KDE ainda não está disponível, mas está sendo elaborado.

OpenVPN
: Para usar esta tecnologia VPN, instale

    - `NetworkManager-openvpn` e
    - `NetworkManager-openvpn-kde4` ou `NetworkManager-openvpn-gnome`.

vpnc (Cisco)
: Para usar esta tecnologia VPN, instale

    - `NetworkManager-vpnc` e
    - `NetworkManager-vpnc-kde4` ou `NetworkManager-vpnc-gnome`.

PPTP (Point-to-Point Tunneling Protocol)
: Para usar esta tecnologia VPN, instale

    - `NetworkManager-pptp` e

- `NetworkManager-pptp-kde4` ou `NetworkManager-pptp-gnome`.

Após instalar os pacotes, configure sua conexão VPN conforme descrito no Seção 26.3, “Configurando conexões de rede” (p 381).

26.7 NetworkManager e segurança

O NetworkManager distingue dois tipos de conexões wireless: confiáveis e não confiáveis. Uma conexão confiável é qualquer rede selecionada explicitamente no passado. Todas as outras são não confiáveis. As conexões confiáveis são identificadas pelo nome e pelo endereço MAC do ponto de acesso. O uso do endereço MAC garante que você não possa usar um ponto de acesso diferente com o nome da conexão confiável.

O NetworkManager faz uma exploração periódica de redes wireless disponíveis. Se forem encontradas várias redes confiáveis, a usada mais recentemente será selecionada automaticamente. O NetworkManager aguarda a sua seleção caso nenhuma das redes seja confiável.

Se a configuração de criptografia mudar, mas o nome e o endereço MAC continuarem os mesmos, o NetworkManager tentará se conectar, mas primeiro você será solicitado a confirmar as novas configurações de criptografia e fornecer atualizações, como uma nova chave.

Se você mudar da conexão wireless para o modo offline, o NetworkManager deixará o SSID ou o ESSID em branco. Isso garante que a placa seja desconectada.

26.7.1 Conexões de usuário e sistema

O NetworkManager conhece dois tipos de conexões: conexões de `usuário` e `sistema`. As conexões de usuário são aquelas que ficam disponíveis ao NetworkManager quando o primeiro usuário efetua login. Quaisquer credenciais necessárias são solicitadas ao usuário e, quando ele efetua logout, as conexões são desconectadas e removidas do NetworkManager. As conexões definidas como sendo de sistema podem ser compartilhadas por todos os usuários e disponibilizadas logo após o NetworkManager ser iniciado, antes que qualquer usuário efetue login. No caso das conexões do sistema, todas as credenciais devem ser fornecidas no momento em que

a conexão é criada. Tais conexões do sistema podem ser usadas para conectar-se automaticamente a redes que exigem autorização. Para obter informações sobre como configurar conexões de usuário ou de sistema com o NetworkManager, consulte a Seção 26.3, “Configurando conexões de rede” (p 381).

No KDE, a configuração de conexões do sistema com o NetworkManager não é suportada (em vez disso, use o YaST).

26.7.2 Armazenando senhas e credenciais

Se você não quiser digitar novamente suas credenciais toda vez que se conectar a uma rede criptografada, use as ferramentas específicas de área de trabalho Gerenciador de Chaves do GNOME ou KWalletManager para armazenar suas credenciais criptografadas no disco, protegidas por uma senha master.

No KDE, é possível configurar se e como armazenar suas credenciais. Para fazer isso, clique no ícone do NetworkManager e selecione *Gerenciar Conexões*. Clique em *Outro* > *Segredos da Conexão* e selecione uma das seguintes opções:

Não Armazenar (Perguntar Sempre)
: Isso é útil quando você está trabalhando em um ambiente onde o armazenamento de credenciais é considerado um risco de segurança.

No Arquivo (Sem Encriptação)
: Se você escolher essa opção, suas senhas serão armazenadas sem criptografia no respectivo arquivo de conexão criado para cada conexão. Eles se encontram em `$HOME/.kde4/share/apps/networkmanagement/connections`.

> **ATENÇÃO: risco de segurança**
>
> Armazenar suas credenciais de rede sem criptografia é um risco de segurança. Todos que acessam o seu computador podem reutilizar a sua conectividade e interceptar sua conexão de rede.

Em Armazenamento Seguro (Criptografado)
: Se você escolher essas opções, suas credenciais serão armazenadas no KWalletManager. Para obter mais informações sobre o KWalletManager, consulte o Chapter 8, *Managing Passwords with KWallet Manager* (↑*KDE User Guide*).

O NetworkManager também pode recuperar seus certificados para conexões seguras (por exemplo, conexões com fio, wireless ou VPN criptografadas) do armazenamento de certificado. Para obter mais informações, consulte o Chapter 12, *Certificate Store* (↑*Security Guide*).

26.8 Perguntas mais frequentes

Veja a seguir algumas perguntas frequentes sobre a configuração de opções de rede especiais com o NetworkManager.

Como vincular uma conexão a um dispositivo específico?
: Por padrão, as conexões no NetworkManager são específicas ao tipo de dispositivo: elas se aplicam a todos os dispositivos físicos do mesmo tipo. Se houver mais de um dispositivo físico disponível por tipo de conexão (por exemplo, quando a máquina está equipada com duas placas ethernet), você poderá vincular uma conexão a um determinado dispositivo.

  Para fazer isso no GNOME, primeiro procure o endereço MAC do seu dispositivo (use as *Informações da Conexão* disponíveis no applet ou use a saída das ferramentas de linha de comando, como `nm-tool` ou `ifconfig`). Em seguida, inicie a caixa de diálogo para configurar conexões de rede e escolher a conexão que você deseja modificar. Na guia *Com fio* ou *Wireless*, digite o *Endereço MAC* do dispositivo e confirme suas mudanças.

  Se estiver usando o KDE, inicie a caixa de diálogo para configurar as conexões de rede e escolha a conexão que deseja modificar. Na guia *Ethernet* ou *Wireless*, use a opção *Restringir à Interface* para selecionar a interface de rede à qual vincular a conexão.

Como especificar um determinado ponto de acesso caso sejam detectados vários pontos de acesso com o mesmo ESSID?
: Quando há vários pontos de acesso disponíveis com bandas wireless diferentes (a/b/g/n), o ponto de acesso com o sinal mais forte é automaticamente escolhido por padrão. Para anular isso, use o campo *BSSID* ao configurar conexões wireless.

  O BSSID (Basic Service Set Identifier) identifica de forma exclusiva cada Conjunto de Serviços Básicos. Em um Conjunto de Serviços Básicos de infraestrutura, o BSSID é o endereço MAC do ponto de acesso wireless. Em um Conjunto de

Serviços Básicos independente (ad-hoc), o BSSID é um endereço MAC administrado localmente, gerado de um número aleatório de 46 bits.

Inicie a caixa de diálogo para configurar conexões de rede conforme descrito na Seção 26.3, "Configurando conexões de rede" (p 381). Escolha a conexão wireless que você deseja modificar e clique em *Editar*. Na guia *Wireless*, digite o BSSID.

Como compartilhar conexões de rede com outros computadores?

O dispositivo principal (que está conectado à Internet) não precisa de nenhuma configuração especial. Entretanto, você deve configurar o dispositivo que está conectado ao barramento local ou à máquina, conforme a seguir:

1. Inicie a caixa de diálogo para configurar conexões de rede conforme descrito na Seção 26.3, "Configurando conexões de rede" (p 381). Escolha a conexão que você deseja modificar e clique em *Editar*. Se você estiver usando o GNOME, alterne para a guia *Configurações IPv4* e, na lista suspensa *Método*, escolha *Compartilhado com outros computadores*. Se estiver usando o KDE, alterne para a guia *Endereço IP* e, na lista suspensa *Configurar*, escolha *Compartilhado*. Isso habilitará o encaminhamento de tráfego IP e executar um servidor DHCP no dispositivo. Confirme suas mudanças no NetworkManager.

2. Como o servidor DCHP utiliza a porta `67`, verifique se ela não está bloqueada pelo firewall: Na máquina que compartilha as conexões, inicie o YaST e selecione *Segurança e Usuários* > *Firewall*. Alterne para a categoria *Serviços Permitidos*. Se o *Servidor DCHP* ainda não for exibido como *Serviço Permitido*, selecione *Servidor DCHP* em *Serviços a Permitir* e clique em *Adicionar*. Confirme as mudanças no YaST.

Como fornecer informações de DNS estático com endereços automáticos (DHCP, PPP, VPN)?

Caso um servidor DHCP forneça informações (e/ou rotas) inválidas de DNS, você pode anulá-las. Inicie a caixa de diálogo para configurar conexões de rede conforme descrito na Seção 26.3, "Configurando conexões de rede" (p 381). Escolha a conexão que você deseja modificar e clique em *Editar*. Se você estiver usando o GNOME, alterne para a guia *Configurações IPv4* e, na lista suspensa *Método*, escolha *Somente endereços (DHCP) automáticos*. Se você estiver usando o KDE, passe para a guia *Endereço IP* e, na lista suspensa *Configurar*, escolha *Somente endereços (DHCP) automáticos*. Digite as informações de DNS nos campos *Servidores DNS* e *Domínios de Pesquisa*. Para *Ignorar as rotas obtidas automaticamente*, clique em *Rotas* (GNOME) e ative a respectiva caixa de seleção ou, na lista suspensa na parte inferior

da guia (KDE), selecione *Rotas* e ative a respectiva caixa de seleção. Confirme as mudanças.

Como fazer o NetworkManager conectar-se a redes protegidas por senha antes que um usuário efetue login?

Defina uma `conexão do sistema` que possa ser usada para esse fim. Para obter mais informações, consulte a Seção 26.7, "NetworkManager e segurança" (p 393).

26.9 Solução de problemas

Podem ocorrer problemas de conexão. Alguns problemas comuns relacionados ao NetworkManager são: o applet não é iniciado ou opção ausente na VPN. Métodos para resolver e evitar esses problemas dependem da ferramenta usada.

O applet da área de trabalho do NetworkManager não é iniciado

Os applets GNOME e KDE para NetworkManager serão iniciados automaticamente se a rede for configurada para controle do NetworkManager. Se o applet não for iniciado, verifique se o NetworkManager está habilitado no YaST, conforme descrito na Seção 26.2, "Habilitando ou desabilitando o NetworkManager" (p 380). Em seguida, verifique se o pacote apropriado para o seu ambiente de área de trabalho também está instalado. Se você usa o KDE 4, o pacote é `NetworkManager-kde4`. Para usuários do GNOME, o pacote é `NetworkManager-gnome`.

Se o applet da área de trabalho estiver instalado, mas não for executado por alguma razão, inicie-o manualmente. Se o applet de área de trabalho estiver instalado, mas não estiver em execução por algum motivo, inicie-o manualmente com o comando `nm-applet` (GNOME) ou `knetworkmanager` (KDE).

O applet do NetworkManager não inclui a opção VPN

O suporte a NetworkManager, applets e VPN para NetworkManager é distribuído em pacotes separados. Se o applet NetworkManager não incluir a opção VPN, verifique se os pacotes com suporte ao NetworkManager referentes à sua tecnologia VPN estão instalados. Para obter mais informações, consulte a Seção 26.6, "NetworkManager e VPN" (p 392).

Nenhuma conexão de rede disponível
: Se você configurou sua conexão de rede corretamente e todos os outros componentes para a conexão de rede (roteador etc.) também estiverem em funcionamento, pode ser útil reiniciar as interfaces de rede no seu computador. Para isso, efetue login em uma linha de comando como `root` e execute `rcnetwork restart`.

26.10 Para obter mais informações

Você encontra mais informações sobre o NetworkManager nos seguintes sites na Web e diretórios:

Página do Projeto NetworkManager
: http://projects.gnome.org/NetworkManager/

Front end KDE para NetworkManager
: http://userbase.kde.org/NetworkManagement

Documentação do pacote
: Verifique também o conteúdo dos seguintes diretórios para obter as informações mais recentes sobre o NetworkManager e os applets GNOME e KDE para NetworkManager:

  - `/usr/share/doc/packages/NetworkManager/`,
  - `/usr/share/doc/packages/NetworkManager-kde4/` e
  - `/usr/share/doc/packages/NetworkManager-gnome/`.

Samba 27

Com o Samba, uma máquina Unix pode ser configurada como um servidor de arquivos e de impressão para máquinas Mac OS X, Windows e OS/2. O Samba se tornou um produto completo e bastante complexo. Configure o Samba com o YaST, o SWAT (uma interface da Web) ou editando o arquivo de configuração manualmente.

27.1 Terminologia

A seguir são apresentados alguns termos usados na documentação do Samba e no módulo YaST.

Protocolo SMB
: O Samba usa o protocolo SMB (bloco de mensagens do servidor), que é baseado nos serviços NetBIOS. A Microsoft lançou o protocolo para que outros fabricantes de software pudessem estabelecer conexões com uma rede de domínio Microsoft. Com o Samba, o protocolo SMB opera acima do protocolo TCP/IP, de modo que este último precisa estar instalado em todos os clientes.

Protocolo CIFS
: O protocolo CIFS (sistema de arquivos da Internet comuns) é outro protocolo que possui suporte no Samba. O CIFS é um protocolo de acesso padrão a sistemas de arquivos remotos para utilização pela rede, permitindo que grupos de usuários trabalhem juntos e compartilhem documentos pela rede.

NetBIOS
NetBIOS é uma interface de software (API) projetada para a comunicação entre máquinas que fornecem serviço de nomes. Ele permite que máquinas conectadas à rede reservem nomes para si. Após a reserva, essas máquinas podem ser tratadas pelo nome. Não há um processo central para a verificação de nomes. Qualquer máquina da rede pode reservar quantos nomes quiser, contanto que os nomes não estejam em uso ainda. A interface NetBIOS pode ser implementada para diferentes arquiteturas de rede. Uma implementação que funciona com relativa proximidade com o hardware da rede é chamada de NetBEUI, mas ela muitas vezes é chamada de NetBIOS. Os protocolos de rede implementados com o NetBIOS são o IPX da Novell (NetBIOS via TCP/IP) e TCP/IP.

Os nomes de NetBIOS enviados por TCP/IP não possuem nada em comum com os nomes usados em `/etc/hosts` ou com os nomes definidos pelo DNS. O NetBIOS usa sua própria convenção de nomes independente. Contudo, é recomendável usar nomes que correspondam aos nomes de hosts DNS para facilitar a administração ou usar o DNS nativamente. Esse é o padrão usado pelo Samba.

Servidor Samba
O servidor Samba fornece serviços SMB/CIFS e serviços de nomeação NetBIOS por IP aos clientes. Para o Linux, existem três daemons para servidor Samba: smbd para serviços SMB/CIFS, nmbd para serviços de nomeação e winbind para autenticação.

Cliente Samba
O cliente Samba é um sistema que usa serviços Samba de um servidor Samba pelo protocolo SMB. Todos os sistemas operacionais comuns, como Mac OS X, Windows e OS/2, prestam suporte ao protocolo SMB. O protocolo TCP/IP precisa estar instalado em todos os computadores. O Samba fornece um cliente para as diferentes versões do UNIX. No caso do Linux, há um módulo de kernel para SMB que permite a integração de recursos SMB no nível de sistema Linux. Não é necessário executar nenhum daemon para o cliente Samba.

Compartilhamentos
Os servidores SMB oferecem recursos aos clientes por meio de compartilhamentos. Compartilhamentos são impressoras e diretórios com seus subdiretórios no servidor. Ele é exportado por meio de um nome e pode ser acessado pelo nome. O nome do compartilhamento pode ser definido por qualquer nome; não precisa ser o nome do diretório de exportação. Uma impressora também recebe um nome. Os clientes podem acessar a impressora pelo nome.

DC
: Um controlador de domínio (DC) é um servidor que gerencia contas em domínios. Para a replicação de dados, os controladores de domínio adicionais estão disponíveis em um domínio.

27.2 Configurando um servidor Samba

Para configurar um servidor Samba, consulte a documentação do SUSE Linux Enterprise Server.

27.3 Configurando clientes

Os clientes somente podem acessar o servidor Samba via TCP/IP. O NetBEUI e o NetBIOS via IPX não podem ser usados com o Samba.

27.3.1 Configurando um cliente Samba com o YaST

Configure um cliente Samba para acessar recursos (arquivos ou impressoras) no servidor Samba ou Windows. Digite o domínio NT ou Active Directory ou o grupo de trabalho na caixa de diálogo *Serviços de Rede > Participação no Domínio do Windows*. Se você ativar *Também Usar Informação SMB para Autenticação Linux*, a autenticação do usuário será executada no servidor Samba, NT ou Kerberos.

Clique em *Configurações de Especialista* para ver as opções de configuração avançadas. Por exemplo, use a tabela *Montar Diretórios do Servidor* para habilitar a montagem de diretório pessoal do servidor automaticamente com autenticação. Assim os usuários poderão acessar seus diretórios pessoais quando estiverem hospedados no CIFS. Para ver os detalhes, consulte a página de manual de `pam_mount`.

Após concluir todas as configurações, confirme a caixa de diálogo para terminar a configuração.

27.4 Samba como servidor de login

Em redes onde se encontram predominantemente clientes Windows, muitas vezes é preferível que os usuários somente possam se registrar com uma conta e senha válidos. Em uma rede baseada no Windows, essa tarefa é gerenciada por um PDC (primary domain controller — controlador de domínio primário). Você pode usar um servidor Windows NT configurado como PDC, mas essa tarefa também pode ser executada com um servidor Samba. As entradas a serem feitas na seção `[global]` de `smb.conf` aparecem em Exemplo 27.1, "Seção global em smb.conf" (p 402).

***Exemplo 27.1** Seção global em smb.conf*

```
[global]
    workgroup = TUX-NET
    domain logons = Yes
    domain master = Yes
```

Se forem usadas senhas criptografadas para fins de verificação, os servidores Samba devem ser capazes de gerenciá-las. A entrada `encrypt passwords = yes` na seção `[global]` permite isso (com a versão 3 do Samba, esse passa a ser o padrão). Além disso, é necessário preparar contas e senhas de usuários em formato de criptografia compatível com o Windows. Para isso, use o comando `smbpasswd -a name`. Crie a conta de domínio dos computadores, exigida pelo conceito de domínio do Windows , com os seguintes comandos:

```
useradd hostname\$
smbpasswd -a -m hostname
```

Com o comando `useradd`, um símbolo de cifrão é adicionado. O comando `smbpasswd` insere esse símbolo automaticamente quando o parâmetro `-m` é usado. O exemplo de configuração comentado (`/usr/share/doc/packages/samba/examples/smb.conf.SUSE`) contém configurações que automatizam essa tarefa.

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$
```

Para certificar-se de que o Samba possa executar esse script corretamente, escolha um usuário do Samba com as permissões de administrador necessárias e adicione-o ao grupo `ntadmin`. Em seguida, será possível atribuir a todos os usuários pertencentes a esse grupo Linux o status de `Domain Admin` com o comando:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Para obter mais informações sobre este tópico, consulte o Capítulo 12 do HOWTO do Samba 3, encontrado em `/usr/share/doc/packages/samba/Samba3-HOWTO.pdf`.

27.5 Para obter mais informações

Informações detalhadas sobre o Samba estão disponíveis na documentação digital. Para obter mais documentação e exemplos online, digite `apropos samba` na linha de comando para exibir algumas páginas de manual ou simplesmente pesquise no diretório `/usr/share/doc/packages/samba`, se a documentação do Samba estiver instalada. Um exemplo de configuração comentado (`smb.conf.SUSE`) encontra-se no subdiretório `examples`.

O HOWTO do Samba 3, fornecido pela equipe Samba, inclui uma seção sobre a solução de problemas. Além disso, a Parte V do documento oferece um guia passo a passo para a verificação da configuração. O HOWTO do Samba 3 poderá ser encontrado em `/usr/share/doc/packages/samba/Samba3-HOWTO.pdf` após a instalação do pacote `samba-doc`.

Compartilhando sistemas de arquivos com o NFS 28

Distribuir e compartilhar sistemas de arquivos em uma rede é uma tarefa comum em ambientes corporativos. O reconhecido sistema de arquivos de rede (*NFS*) funciona com o *NIS*, o protocolo de yellow pages. Para um protocolo mais seguro que funcione com o *LDAP* e também possa usar Kerberos, marque *NFSv4*. Juntamente com o pNFS, é possível eliminar gargalos no desempenho.

O NFS com o NIS torna uma rede transparente para o usuário. Com o NFS, é possível distribuir sistemas de arquivos arbitrários pela rede. Com a configuração adequada, os usuários sempre ficam no mesmo ambiente, independentemente do terminal que estejam usando.

28.1 Terminologia

Veja a seguir os termos usados no módulo do YaST.

Exportações
: Um diretório *exportado* por um servidor NFS, que os clientes podem integrar a seus sistemas.

Cliente NFS
: O cliente NFS é um sistema que usa serviços NFS de um servidor NFS pelo protocolo NFS (Network File System – Sistema de Rede de Arquivos). O protocolo TCP/IP já está integrado ao kernel do Linux; não há necessidade de instalar software adicional.

Servidor NFS
: O servidor NFS fornece serviços NFS aos clientes. Um servidor em execução depende dos seguintes daemons: `nfsd` (worker), `idmapd` (mapeamentos de nome de grupo e usuário para IDs e vice versa), `statd` (bloqueio de arquivos) e `mountd` (solicitações de montagem).

pNFS
: NFS Paralelo, o protocolo de extensão do NFSv4. Qualquer cliente do pNFS pode acessar diretamente os dados em um servidor NFS.

28.2 Instalando o servidor NFS

O software do servidor NFS não faz parte da instalação padrão. Se você configurar um servidor NFS conforme descrito na Seção 28.3, "Configurando o servidor NFS" (p 406), receberá automaticamente um aviso solicitando para instalar os pacotes necessários. Se preferir, instale o pacote `nfs-kernel-server` com o YaST ou o zypper.

Assim como o NIS, o NFS é um sistema cliente/servidor. Porém, uma máquina pode ser ambos, ou seja, fornecer sistemas de arquivos pela rede (exportar) e montar sistemas de arquivos de outros hosts (importar).

28.3 Configurando o servidor NFS

É possível configurar um servidor NFS usando o YaST ou manualmente. Para autenticação, o NFS também pode ser combinado com o Kerberos.

28.3.1 NFS com Kerberos

Para usar a autenticação Kerberos para o NFS, é preciso que a segurança GSS esteja habilitada. Selecione *Habilitar Segurança GSS* na caixa de diálogo inicial Servidor NFS do YaST. É preciso ter um servidor Kerberos ativo para usar esse recurso. O YaST não configura o servidor, apenas usa a funcionalidade disponível. Para usar a autenticação Kerberos além da configuração do YaST, conclua pelo menos as etapas seguintes antes de executar a configuração do NFS:

1. Verifique se o servidor e o cliente estão no mesmo domínio Kerberos. Eles precisam acessar o mesmo servidor KDC (Key Distribution Center — Centro de Distribuição de Chaves) e compartilhar o arquivo `krb5.keytab` (o local padrão em qualquer máquina é `/etc/krb5.keytab`). Para obter mais informações sobre o Kerberos, consulte o Chapter 6, *Network Authentication with Kerberos* (↑*Security Guide*).

2. Inicie o serviço gssd no cliente com `rcgssd start`.

Para obter mais informações sobre como configurar o NFS que usa Kerberos, consulte os links na Seção 28.5, “Para obter mais informações” (p 411).

28.4 Configurando clientes

Para configurar seu host como cliente NFS, você não precisa instalar software adicional. Todos os pacotes necessários são instalados por padrão.

28.4.1 Importando sistemas de arquivos com o YaST

Usuários autorizados podem montar diretórios NFS de um servidor NFS na árvore de arquivos local usando o módulo de cliente NFS do YaST. Proceda da seguinte maneira:

Procedimento 28.1 *Importando diretórios NFS*

1. Inicie o módulo de cliente NFS do YaST.

2. Clique em *Adicionar* na guia *Compartilhamentos NFS*. Digite o nome de host do servidor NFS, o diretório a ser importado e o ponto de montagem desse diretório localmente.

3. Habilite *Abrir Porta no Firewall* na guia *Configurações do NFS*, se você usa um Firewall e deseja permitir o acesso de computadores remotos ao serviço. O status do firewall é mostrado próximo à caixa de seleção.

4. Ao usar NFSv4, verifique se a caixa de seleção *Habilitar NFSv4* está marcada e se o *Nome de Domínio NFSv4* inclui o mesmo valor usado pelo servidor NFSv4. O domínio padrão é `localdomain`.

5 Clique em *OK* para gravar as mudanças.

A configuração é gravada em `/etc/fstab` e os sistemas de arquivos especificados são montados. Quando você iniciar o cliente de configuração do YaST posteriormente, ele também lerá a configuração existente desse arquivo.

28.4.2 Importando sistemas de arquivos manualmente

O pré-requisito para importar os sistemas de arquivos manualmente de um servidor NFS é um mapeador de portas RPC em execução. Comece digitando `rcrpcbind start` enquanto usuário `root`. Em seguida, os sistemas de arquivos remotos podem ser montados no sistema de arquivos como partições locais usando `mount`:

```
mount host:remote-pathlocal-path
```

Para importar os diretórios de usuário da máquina do `nfs.example.com`, por exemplo, use:

```
mount nfs.example.com:/home /home
```

28.4.2.1 Usando o serviço de montagem automática

O daemon autofs pode ser usado para montar sistemas de arquivos remotos automaticamente. Adicione a seguinte entrada ao seu arquivo `/etc/auto.master`:

```
/nfsmounts /etc/auto.nfs
```

Agora, o diretório `/nfsmounts` atuará como raiz para todas as montagens NFS no cliente se o arquivo `auto.nfs` for preenchido adequadamente. O nome `auto.nfs` foi escolhido por mera conveniência, você pode escolher qualquer nome. Adicione entradas ao `auto.nfs` para todas as montagens NFS da seguinte maneira:

```
localdata -fstype=nfs server1:/data
nfs4mount -fstype=nfs4 server2:/
```

Ative as configurações com `rcautofs start` como `root`. Neste exemplo, `/nfsmounts/localdata`, o diretório `/data` do `server1`, é montado com NFS e `/nfsmounts/nfs4mount`, do `server2`, é montado com NFSv4.

Se o arquivo /etc/auto.master for editado enquanto o serviço autofs estiver em execução, o automontador deverá ser reiniciado com rcautofs restart para que as mudanças tenham efeito.

28.4.2.2 Editando /etc/fstab manualmente

Uma entrada de montagem típica do NFSv3 em /etc/fstab tem aparência semelhante a esta:

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

As montagens NFSv4 também podem ser adicionadas ao arquivo /etc/fstab. Para essas montagens, use nfs4 em vez de nfs na terceira coluna e verifique se o sistema de arquivos remoto aparece como / após *nfs.example.com:* na primeira coluna. Uma linha de amostra de uma montagem NFSv4 em /etc/fstab tem aparência semelhante a esta:

```
nfs.example.com:/ /local/pathv4 nfs4 rw,noauto 0 0
```

A opção noauto impede que o sistema de arquivos seja montado automaticamente na inicialização. Se desejar montar o respectivo sistema de arquivos manualmente, é possível abreviar o comando de montagem especificando apenas o ponto de montagem:

```
mount /local/path
```

Observe que, se você não digitar a opção noauto, os scripts de inicialização do sistema gerenciarão a montagem dos sistemas de arquivos na inicialização.

28.4.3 NFS paralelo (pNFS)

NFS é um dos protocolos mais antigos, desenvolvido nos anos 80. Em geral, o NFS é suficiente para compartilhar arquivos pequenos. Entretanto, para transferir arquivos grandes ou quando um número elevado de clientes precisa acessar os dados, o servidor NFS torna-se um gargalo e afeta significativamente o desempenho do sistema. Isso ocorre porque os arquivos aumentam de tamanho rapidamente, mas a velocidade relativa do Ethernet não consegue acompanhar esse aumento.

Quando você solicita um arquivo de um servidor NFS “normal”, o servidor procura os metadados do arquivo, coleta todos os dados e os transfere pela rede até o cliente. No

entanto, o gargalo no desempenho torna-se aparente independentemente do tamanho dos arquivos:

- Com os arquivos pequenos, a maior parte do tempo é gasta para coletar os metadados
- Com os arquivos grandes, a maior parte do tempo é gasta para transferir os dados do servidor para o cliente

O pNFS, ou NFS paralelo, supera essa limitação, pois ele separa os metadados do sistema de arquivos do local dos dados. Para isso, o pNFS requer dois tipos de servidores:

- Um *servidor de controle* ou de *metadados* que controla todo o tráfego que não seja de dados
- Um ou mais *servidor(es) de armazenamento* que armazena(m) os dados

Os servidores de metadados e de armazenamento formam um único servidor NFS lógico. Para o cliente ler ou gravar, o servidor de metadados informa ao cliente NFSv4 qual servidor de armazenamento deve ser usado para acessar os pacotes de arquivos. O cliente pode acessar os dados diretamente no servidor.

O SUSE Linux Enterprise suporta pNFS apenas no cliente.

28.4.3.1 Configurando o cliente pNFS com o YaST

Siga a descrição no Procedimento 28.1, “Importando diretórios NFS” (p 407), mas clique na caixa de seleção *pNFS (v4.1)* e, opcionalmente, em *Compartilhamento NFSv4*. O YaST executa todas as etapas necessárias e grava todas as opções exigidas no arquivo `/etc/exports`.

28.4.3.2 Configurando o cliente pNFS manualmente

Para começar, consulte a Seção 28.4.2, “Importando sistemas de arquivos manualmente” (p 408). A maior parte da configuração é feita pelo servidor NFSv4. Para o pNFS, a única diferença é adicionar a opção `minorversion` e o servidor de metadados *`MDS_SERVER`* ao comando `mount`:

```
mount -t nfs4 -o minorversion=1 MDS_SERVER MOUNTPOINT
```

Para ajudar na depuração, mude o valor no sistema de arquivos `/proc`:

```
echo 32767 > /proc/sys/sunrpc/nfsd_debug
echo 32767 > /proc/sys/sunrpc/nfs_debug
```

28.5 Para obter mais informações

Além das páginas de manual de `exports`, `nfs` e `mount`, há informações disponíveis sobre como configurar servidores e clientes NFS em `/usr/share/doc/packages/nfsidmap/README`. Para mais documentações online, consulte os seguintes sites na Web:

- A documentação técnica online encontra-se no SourceForge [`http://nfs.sourceforge.net/`].
- Para obter instruções sobre como configurar o NFS que usa Kerberos, consulte o documento NFS Version 4 Open Source Reference Implementation [`http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html`] (Implementação da referência de código-fonte aberto do NFSv4).
- Se você tiver dúvidas sobre o NFSv4, consulte as Perguntas frequentes do Linux NFSv4 [`http://www.citi.umich.edu/projects/nfsv4/linux/faq/`].

29 Sincronização de arquivos

Atualmente, muitas pessoas usam vários computadores: um em casa, um ou mais computadores no local de trabalho e possivelmente um laptop, tablet ou smartphone em trânsito. Vários arquivos são necessários em todos esses computadores. Talvez você queira trabalhar com todos os computadores e modificar os arquivos, de modo que a versão mais recente dos dados fique disponível em todos os computadores.

29.1 Software de sincronização de dados disponível

A sincronização de dados não é um problema para computadores permanentemente conectados por uma rede rápida. Nesse caso, use um sistema de arquivos de rede, como o NFS, e armazene os arquivos em um servidor para que todos os hosts acessem os mesmos dados via rede. Essa abordagem será impossível se a conexão de rede for instável ou não permanente. Quando você viaja com um laptop, precisa ter cópias de todos os arquivos necessários no disco rígido local. Entretanto, é necessário sincronizar os arquivos modificados. Quando você modificar um arquivo em um computador, verifique se uma cópia dele foi atualizada em todos os outros computadores. No caso de cópias ocasionais, elas podem ser feitas manualmente com o scp ou o rsync. Entretanto, se vários arquivos forem envolvidos, o procedimento poderá ser complicado e demandar muito cuidado para evitar erros, como a sobregravação de um arquivo novo por um antigo.

ATENÇÃO: risco de perda de dados

Antes de começar a gerenciar seus dados com um sistema de sincronização, você deve se informar sobre o programa usado e testar sua funcionalidade. É indispensável ter um backup de arquivos importantes.

A tarefa prolongada e sujeita a erros de sincronizar dados manualmente pode ser evitada se você usar um dos programas que utilizam vários métodos para automatizá-la. Os resumos a seguir têm o simples objetivo de dar uma visão geral sobre como esses programas funcionam e como podem ser usados. Se você planeja usá-los, leia a documentação do programa.

29.1.1 CVS

O CVS, que é mais usado para gerenciar versões de origem de programas, oferece a possibilidade de manter cópias dos arquivos em vários computadores. Dessa forma, ele também é adequado para sincronização de dados. O CVS mantém um repositório central no servidor, no qual os arquivos e as mudanças feitas neles são gravados. As mudanças realizadas localmente são enviadas para o repositório e podem ser recuperadas de outros computadores por meio de uma atualização. Todos os procedimentos devem ser iniciados pelo usuário.

O CVS é muito suscetível a erros quando ocorrem mudanças em vários computadores. As mudanças são fundidas e, se ocorrerem nas mesmas linhas, um conflito será reportado. Quando ocorre um conflito, o banco de dados permanece em estado consistente. O conflito só fica visível para resolução no host cliente.

29.1.2 rsync

Quando o controle de versão não é necessário, mas grandes estruturas de diretório precisam ser sincronizadas em conexões de rede lentas, a ferramenta rsync oferece mecanismos avançados para a transmissão apenas de mudanças entre arquivos. Isso não diz se aplica apenas a arquivos de texto, mas também a arquivos binários. Para detectar as diferenças entre os arquivos, o rsync os subdivide em blocos e realiza checksums neles.

O esforço dedicado à detecção das mudanças tem um preço. Os sistemas a serem sincronizados devem ser dimensionados generosamente para uso do rsync. A RAM é especialmente importante.

29.2 Determinando fatores para selecionar um programa

Há alguns fatores importantes a serem considerados ao decidir que programa será usado.

29.2.1 Cliente-servidor versus ponto a ponto

Dois modelos diferentes são comumente usados para distribuir dados. No primeiro modelo, todos os clientes sincronizam seus arquivos com um servidor central. O servidor deve ser acessível a todos os clientes pelo menos ocasionalmente. Esse modelo é usado pelo CVS.

A outra possibilidade é deixar todos os hosts ligados em rede sincronizarem seus dados entre os pontos uns dos outros. O rsync funciona de fato no modo cliente, mas qualquer cliente também pode atuar como servidor.

29.2.2 Portabilidade

O CVS e o rsync também estão disponíveis para muitos outros sistemas operacionais, incluindo vários sistemas Unix e Windows.

29.2.3 Interativo versus automático

No CVS, a sincronização de dados começa manualmente pelo usuário. Isso permite um controle fino dos dados a serem sincronizados e um fácil gerenciamento de conflitos. No entanto, se os intervalos de sincronização forem muito longos, será mais provável que ocorram conflitos.

29.2.4 Conflitos: incidência e solução

Conflitos só ocorrem raramente no CVS, mesmo quando há muitas pessoas trabalhando em um grande projeto de programa. Isso ocorre porque os documentos são fundidos na base de linhas individuais. Quando ocorre um conflito, somente um cliente é afetado. Normalmente, os conflitos no CVS podem ser facilmente resolvidos.

Não há gerenciamento de conflitos no rsync. O usuário é responsável por não sobregravar acidentalmente arquivos e resolver manualmente todos os possíveis conflitos. Para fins de segurança, é possível empregar adicionalmente um sistema de controle de versão como o RCS.

29.2.5 Selecionando e adicionando arquivos

No CVS, diretórios e arquivos novos devem ser adicionados explicitamente com o comando `cvs add`. Esse procedimento resulta em um maior controle do usuário sobre os arquivos a serem sincronizados. Por outro lado, novos arquivos são sempre ignorados, especialmente quando os pontos de interrogação na saída de `cvs update` são ignorados devido ao grande número de arquivos.

29.2.6 Histórico

Um recurso adicional do CVS é a possibilidade de reconstrução de versões antigas de arquivos. Um breve comentário de edição pode ser inserido em cada mudança, e o desenvolvimento dos arquivos pode ser facilmente rastreado posteriormente com base no conteúdo dos comentários. Essa é uma ajuda valiosa para textos de teses e de programas.

29.2.7 Volume de dados e requisitos do disco rígido

Os discos rígidos de todos os hosts envolvidos devem ter espaço em disco suficiente para todos os dados distribuídos. O CVS requer espaço adicional para o banco de dados de repositório no servidor. O histórico do arquivo também é armazenado no servidor, requerendo ainda mais espaço. Quando arquivos em formato de texto são mudados,

somente as linhas modificadas são gravadas. Arquivos binários requerem espaço em disco adicional relativo ao tamanho do arquivo sempre que ele for mudado.

29.2.8 GUI

Usuários experientes normalmente executam o CVS a partir da linha de comando. Entretanto, há interfaces gráficas do usuário disponíveis para Linux (como a cervisia) e para outros sistemas operacionais (como a wincvs). Muitas ferramentas de desenvolvimento (como a kdevelop) e editores de texto (como o Emacs) fornecem suporte ao CVS. É sempre mais fácil realizar a resolução de conflitos com esses front ends.

29.2.9 Facilidade de uso

O rsync é bastante fácil de usar, sendo também adequado para principiantes. O CVS é um pouco mais difícil de operar. Os usuários devem entender a interação entre o repositório e os dados locais. As mudanças dos dados devem ser primeiro fundidas localmente no repositório. Esse procedimento é feito com o comando `cvs update`. Em seguida, os dados devem ser enviados de volta ao repositório com o comando `cvs commit`. Depois de compreender esse procedimento, os usuários principiantes também serão capazes de usar o CVS com facilidade.

29.2.10 Segurança contra ataques

Durante a transmissão, o ideal é proteger os dados contra interceptação e manipulação. O CVS e o rsync podem ser facilmente usados via ssh (secure shell), fornecendo segurança contra ataques deste tipo. A execução do CVS via rsh (remote shell) deve ser evitada. O acesso ao CVS com o mecanismo *pserver* em redes desprotegidas também não é recomendável.

29.2.11 Proteção contra perda de dados

O CVS tem sido usado por desenvolvedores por um longo tempo para gerenciar projetos de programas e é extremamente estável. Como o histórico do desenvolvimento é gravado,

o CVS fornece proteção até mesmo contra certos erros do usuário, como uma exclusão não intencional de um arquivo.

Tabela 29.1 *Recursos das Ferramentas de Sincronização de Arquivos: -- = muito ruim, - = ruim ou indisponível, o = médio, + = bom, ++ = excelente, x = disponível*

	CVS	**rsync**
Cliente/Servidor	C-S	C-S
Portabilidade	Lin,Un*x,Win	Lin,Un*x,Win
Interatividade	x	x
Velocidade	o	+
Conflitos	++	o
Sel. de arquivos	Sel./arq., dir.	Dir.
Histórico	x	-
Espaço em disco rígido	--	o
Interface gráfica do usuário (GUI)	o	-
Dificuldade	o	+
Ataques	+ (ssh)	+(ssh)
Perda de dados	++	+

29.3 Introdução ao CVS

O CVS é adequado para fins de sincronização, caso arquivos específicos sejam editados com frequência e sejam armazenados em um formato de arquivo, como texto ASCII,

ou como texto de origem de programa. O uso do CVS para sincronizar dados em outros formatos (como arquivos JPEG) é possível, mas gera grandes volumes de dados, pois todas as variantes de um arquivo ficam armazenadas permanentemente no servidor CVS. Nesses casos, não é possível usar a maioria dos recursos do CVS. O uso do CVS para sincronizar arquivos só será possível se todas as estações de trabalho puderem acessar o mesmo servidor.

29.3.1 Configurando um servidor CVS

O *servidor* é o host em que todos os arquivos válidos se localizam, incluindo as versões mais recentes de todos os arquivos. Qualquer estação de trabalho estacionária pode ser usada como um servidor. Se possível, os dados do repositório do CVS devem ser incluídos em backups regulares.

Durante a configuração de um servidor CVS, é uma boa ideia conceder aos usuários o acesso ao servidor via SSH. Se o usuário for conhecido pelo servidor como `tux` e o software do CVS estiver instalado tanto no servidor quanto no cliente, as variáveis de ambiente a seguir deverão ser definidas no lado do cliente:

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

O comando `cvs init` pode ser usado para inicializar o servidor CVS no lado cliente. Esse procedimento deve ser executado apenas uma vez.

Finalmente, é necessário designar um nome à sincronização. Selecione ou crie um diretório no cliente para conter arquivos a serem gerenciados com o CVS (o diretório também pode ficar vazio). O nome do diretório também será o nome da sincronização. Neste exemplo, o diretório é chamado de `synchome`. Vá para esse diretório e digite o comando a seguir para definir o nome de sincronização como `synchome`:

```
cvs import synchome tux wilber
```

Vários comandos do CVS requerem um comentário. Para essa finalidade, o CVS inicia um editor (o editor definido na variável do ambiente `$EDITOR` ou vi, se nenhum editor tiver sido definido). A chamada do editor pode ser evitada se você inserir o comentário antes na linha de comando, como no exemplo a seguir:

```
cvs import -m 'this is a test' synchome tux wilber
```

29.3.2 Usando o CVS

O repositório de sincronização agora pode ter a saída registrada de todos os hosts com `cvs co synchome`. Esse procedimento cria um novo subdiretório `synchome` no cliente. Para confirmar suas mudanças ao servidor, vá para o diretório `synchome` (ou um de seus subdiretórios) e digite `cvs commit`.

Por padrão, todos os arquivos (incluindo subdiretórios) são confirmados no servidor. Para confirmar apenas determinados arquivos ou diretórios individuais, especifique-os como em `cvs commit arquivo1 diretório1`. É necessário adicionar novos arquivos e diretórios ao repositório com um comando como `cvs add arquivo1 diretório1` antes de confirmá-los no servidor. Depois disso, confirme os arquivos e diretórios recém-adicionados com `cvs commit arquivo1 diretório1`.

Se você for para outra estação de trabalho, registre a saída do repositório de sincronização, caso isso não tenha sido feito em uma sessão anterior na mesma estação de trabalho.

Inicie a sincronização com o servidor com `cvs update`. Atualize arquivos ou diretórios individuais como em `cvs update arquivo1 diretório1`. Para ver a diferença entre os arquivos atuais e versões armazenadas no servidor, use o comando `cvs diff` ou `cvs diff arquivo1 diretório1`. Use `cvs -nq update` para ver quais arquivos podem ser afetados por uma atualização.

Estes são alguns símbolos de status exibidos durante uma atualização:

U
: A versão local foi atualizada. Isso afeta todos os arquivos fornecidos pelo servidor e ausentes no sistema local.

M
: A versão local foi modificada. Se havia mudanças no servidor, foi possível fundir as diferenças na cópia local.

P
: A versão local foi corrigida com a versão do servidor.

C
: O arquivo local está em conflito com a versão atual do repositório.

?
: Este arquivo não existe no CVS.

O status M indica um arquivo modificado localmente. Envie a cópia local para o servidor ou remova o arquivo local e execute a atualização novamente. Nesse caso, o arquivo ausente será recuperado do servidor. Se você enviar um arquivo modificado localmente e ele tiver sido mudado na mesma linha de comando e enviado, poderá haver um conflito, indicado por C.

Nesse caso, observe as marcas de conflito (“>>” e “<<”) no arquivo e decida-se entre as duas versões. Como essa tarefa pode ser desagradável, você pode abandonar as mudanças, apagar o arquivo local e digitar `cvs up` para recuperar a versão atual do servidor.

29.4 Introdução ao rsync

O rsync será útil quando for necessário transmitir grandes quantidades de dados regularmente, sem que haja muitas mudanças. Esse é, por exemplo, sempre o caso da criação de backups. Uma outra aplicação diz respeito a servidores para teste. Esses servidores armazenam árvores completas de diretório de servidores Web regularmente espelhadas em um servidor Web em um DMZ.

29.4.1 Configuração e operação

O rsync pode ser operado em dois modos diferentes. Ele pode ser usado para arquivar ou copiar dados. Para isso, somente um shell remoto, como o ssh, é necessário no sistema de destino. Entretanto, o rsync também pode ser usado como um daemon para fornecer diretórios à rede.

O modo de operação básica do rsync não requer qualquer configuração especial. O rsync permite diretamente o espelhamento de diretórios inteiros em outro sistema. Como exemplo, o comando a seguir cria um backup do diretório pessoal do tux em um servidor de backup chamado de sun:

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

O comando a seguir é usado para reproduzir o diretório de volta:

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

Até esse ponto, o gerenciamento não é muito diferente do de uma ferramenta de cópia comum, como o scp.

O rsync deve ser operado no modo “rsync” para que todos os recursos fiquem totalmente disponíveis. Isso é feito ao se iniciar o daemon rsyncd em mais de um sistema. Configure-o no arquivo /etc/rsyncd.conf. Por exemplo, para tornar o diretório /srv/ftp disponível com o rsync, use a seguinte configuração:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = An Example
```

Em seguida, inicie o rsyncd com rcrsyncd start. O rsyncd também pode ser iniciado automaticamente durante o processo de boot. Configure esse recurso ativando esse serviço no editor de nível de execução fornecido pelo YaST ou digitando manualmente o comando insserv rsyncd. O rsyncd também pode ser iniciado com xinetd. Entretanto, isso só é recomendável para servidores que raramente usam o rsyncd.

O exemplo também cria um arquivo de registro listando todas as conexões. Esse arquivo é armazenado em /var/log/rsyncd.log.

Então será possível testar a transferência de um sistema cliente. Faça isso com o seguinte comando:

```
rsync -avz sun::FTP
```

Esse comando lista todos os arquivos presentes no diretório /srv/ftp do servidor. Essa solicitação também é registrada no arquivo de registro /var/log/rsyncd.log. Para iniciar uma transferência real, forneça um diretório de destino. Use . para o diretório atual. Por exemplo:

```
rsync -avz sun::FTP .
```

Por padrão, nenhum arquivo será apagado durante a sincronização com o rsync. Se esse procedimento for forçado, a opção adicional --delete deverá ser expressa. Para

garantir que nenhum arquivo novo seja apagado, use a opção `--update` como alternativa. Qualquer conflito ocorrido deve ser resolvido manualmente.

29.5 Para obter mais informações

CVS

Você encontra informações importantes sobre o CVS na home page http://www.cvshome.org.

rsync

Informações importantes sobre o rsync são fornecidas nas páginas de manual `man rsync` e `man rsyncd.conf`. Uma referência técnica sobre os princípios de operação do rsync pode ser encontrada em `/usr/share/doc/packages/rsync/tech_report.ps`. As notícias mais recentes sobre o rsync encontram-se no site do projeto na Web, em http://rsync.samba.org/.

Parte V. Solução de problemas

30 Ajuda e documentação

O SUSE® Linux Enterprise Desktop vem com várias fontes de informações e documentação, muitas das quais já integradas ao sistema instalado.

Documentação em /usr/share/doc
: Esse diretório de ajuda tradicional contém vários arquivos de documentação e notas de versão do seu sistema. Também contém informações de pacotes instalados no subdiretório packages. Mais informações podem ser encontradas na Seção 30.1, "Diretório da documentação" (p 428).

Páginas de manual e páginas de informações para comandos do shell
: Ao trabalhar com o shell, você não precisa saber de cor as opções de comandos. Tradicionalmente, o shell oferece ajuda integrada por meio das páginas de manual e de informações. Leia mais na Seção 30.2, "Páginas de manual" (p 430) e na Seção 30.3, "Páginas de informações" (p 431).

Centros de ajuda da área de trabalho
: Os centros de Ajuda das áreas de trabalho do KDE (Centro de Ajuda do KDE) e do GNOME (Yelp) proporcionam acesso central aos recursos de documentação mais importantes do sistema, de forma pesquisável. Esses recursos incluem Ajuda online para os aplicativos instalados, páginas de manual, páginas de informações e os manuais da Novell/SUSE fornecidos com o produto.

Pacotes de Ajuda separados para alguns aplicativos
: Quando um novo software é instalado com o YaST, a documentação do software é instalada automaticamente (na maioria dos casos) e, normalmente, aparece no centro de ajuda da área de trabalho. Porém, alguns aplicativos, como o GIMP,

podem ter diversos pacotes de ajuda online que podem ser instalados separadamente com o YaST e que não se integram aos centros de ajuda.

30.1 Diretório da documentação

O diretório tradicional para encontrar a documentação do sistema Linux instalado é `/usr/share/doc`. Geralmente, o diretório contém informações sobre os pacotes instalados no sistema, bem como notas de versão, manuais e muito mais.

NOTA: o conteúdo depende dos pacotes instalados

No mundo do Linux, muitos manuais e outros tipos de documentação estão disponíveis na forma de pacotes, assim como um software. As informações encontradas em `/usr/share/docs` também dependem dos pacotes (de documentação) instalados. Se você não encontrar os subdiretórios mencionados aqui, verifique se os respectivos pacotes estão instalados em seu sistema e adicione-os com o YaST, se necessário.

30.1.1 Manuais da Novell/SUSE

Oferecemos as versões em HTML e PDF dos nossos manuais em idiomas diferentes. No subdiretório `manual`, você encontra as versões em HTML de quase todos os manuais da Novell/SUSE disponíveis para o seu produto. Para obter uma visão geral de toda a documentação disponível para o seu produto, consulte o prefácio dos manuais.

Se houver mais de um idioma instalado, `/usr/share/doc/manual` poderá conter versões em idiomas diferentes dos manuais. As versões em HTML dos manuais da Novell/SUSE também estão disponíveis no centro de ajuda de ambas as áreas de trabalho. Para obter informações sobre onde encontrar as versões em PDF e HTML dos manuais na mídia de instalação, consulte as Notas de Versão do SUSE Linux Enterprise Desktop. Elas estão disponíveis no sistema instalado, no diretório `/usr/share/doc/release-notes/`, ou online, na página da Web específica do produto em http://www.suse.com/doc/.

30.1.2 HOWTOs

Se o pacote howto estiver instalado no sistema, /usr/share/doc também conterá o subdiretório howto, no qual você encontra documentação adicional de muitas tarefas relacionadas a configuração e operação do software Linux.

30.1.3 Documentação do pacote

Em packages, você encontra a documentação incluída nos pacotes de software instalados no seu sistema. Para qualquer pacote, é criado um subdiretório /usr/share/doc/packages/*nome_do_pacote*. Ele geralmente contém arquivos README do pacote e às vezes exemplos, arquivos de configuração ou scripts adicionais. A lista a seguir apresenta arquivos típicos encontrados em /usr/share/doc/packages. Nenhuma dessas entradas é obrigatória e muitos pacotes podem incluir apenas alguns deles.

AUTHORS
: Lista dos principais desenvolvedores.

BUGS
: Bugs ou falhas conhecidos. Pode conter também um link para uma página do Bugzilla na Web, onde é possível pesquisar todos os bugs.

CHANGES , ChangeLog
: Resumo de mudanças de versão para versão. Geralmente interessante para desenvolvedores, pois é bastante detalhado.

COPYING , LICENSE
: Informações sobre licenciamento.

FAQ
: Perguntas e respostas coletadas em listas de endereçamento ou grupos de notícias.

INSTALL
: Como instalar esse pacotes no seu sistema. Visto que o pacote já estará instalado no momento em que você ler este arquivo, você poderá ignorar o conteúdo do arquivo com segurança.

`README`, `README.*`
: Informações gerais sobre o software. Por exemplo, a finalidade e o modo de usá-lo.

`TODO`
: Itens ainda não implementados, mas que provavelmente serão no futuro.

`MANIFEST`
: Lista de arquivos com um breve resumo.

`NEWS`
: Descrição do que há de novo nesta versão.

30.2 Páginas de manual

Páginas de manual são uma parte essencial de qualquer sistema Linux. Elas explicam o uso de um comando e todos os parâmetros e opções disponíveis. As páginas de manual podem ser acessadas com `man` seguido do nome do comando, por exemplo, `man ls`.

As páginas de manual são exibidas diretamente no shell. Para navegar nelas, mova-se para cima e para baixo com Page ↑ e Page ↓. Desloque-se entre o início e o fim do documento com Home e End. Conclua esta exibição pressionando Q. Aprenda mais sobre o próprio comando `man` com `man man`. Páginas de manual são classificadas em categorias, como mostrado na Tabela 30.1, “Páginas de manual – categorias e descrições” (p 431) (extraída da página de manual do próprio comando man).

Tabela 30.1 Páginas de manual – categorias e descrições

Número	Descrição
1	Programas executáveis ou comandos de shell
2	Chamadas do sistema (funções fornecidas pelo Kernel)
3	Chamadas de biblioteca (funções em bibliotecas de programas)
4	Arquivos especiais (geralmente encontrados em `/dev`)
5	Convenções e formatos de arquivos (`/etc/fstab`)
6	Jogos
7	Diversos (incluindo convenções e pacotes de macro); por exemplo, man(7), groff(7)
8	Comandos de administração de sistema (geralmente, apenas para `root`)
9	Rotinas de kernel (não padrão)

Cada página de manual consiste em várias partes rotuladas *NAME*, *SYNOPSIS*, *DESCRIPTION*, *SEE ALSO*, *LICENSING* e *AUTHOR*. Pode haver seções adicionais disponíveis, dependendo do tipo de comando.

30.3 Páginas de informações

Páginas de informações são outra fonte importante de informações no sistema. Geralmente, elas são mais detalhadas do que as páginas de manual. Para ver a página

de informações de um determinado comando, digite `info` seguido pelo nome do comando, por exemplo, `info ls`. Você pode procurar uma página de informações com um viewer diretamente no shell e exibir as seções diferentes, denominadas "nós". Use Space para avançar e <— para voltar. Em um nó, você também pode procurar com Page ↑ e Page ↓, mas apenas Space e <— o levarão também para o nó anterior ou subsequente. Pressione Q para sair do modo de visualização. Nem todas as páginas de manual contém uma página de informações e vice-versa.

30.4 Recursos Online

Além das versões online dos manuais da Novell instalados em `/usr/share/doc`, você também pode acessar a documentação e os manuais específicos do produto na Web. Para uma visão geral de toda a documentação disponível referente ao SUSE Linux Enterprise Desktop, visite a página de documentação específica do seu produto na Web em http://www.suse.com/doc/.

Se você estiver pesquisando mais informações relativas ao produto, também poderá consultar os seguintes sites:

Base de dados de suporte técnico da Novell
: A Novell Technical Support Knowledgebase (Base de Informações de Suporte Técnico da Novell) pode ser encontrada em http://www.novell.com/support/. Ela apresenta artigos elaborados como soluções para problemas técnicos com o SUSE Linux Enterprise Desktop.

Fóruns da Novell
: Há vários fóruns em que você pode participar de discussões sobre produtos da Novell. Acesse http://forums.novell.com/ para obter uma lista.

Cool Solutions
: Uma comunidade online, que oferece artigos, dicas, Perguntas e Respostas e ferramentas gratuitas para fazer download: http://www.novell.com/communities/coolsolutions

Documentação do KDE
: Encontre documentação para vários aspectos do KDE adequada para usuários e administradores em http://www.kde.org/documentation/.

Documentação do GNOME
: A documentação para usuários, administradores e desenvolvedores do GNOME está disponível em `http://library.gnome.org/`.

O Projeto de Documentação do Linux
: O TLDP (The Linux Documentation Project — O Projeto de Documentação do Linux) é administrado por uma equipe de voluntários que escrevem a documentação relacionada ao Linux (acesse `http://www.tldp.org`). É provavelmente o recurso de documentação mais completo para Linux. O conjunto de documentos contém tutoriais para iniciantes, mas é direcionado principalmente a usuários experientes e administradores de sistema profissionais. O TLDP publica HOWTOs (Como Fazer), FAQs e guias (manuais) sob uma licença livre. Partes da documentação do TLDP também estão disponíveis no SUSE Linux Enterprise Desktop

Você também pode experimentar mecanismos de busca para fins gerais. Por exemplo, use os termos de pesquisa `ajuda Linux CD-RW` ou `problema de conversão de arquivos OpenOffice` se tiver problemas com a gravação de CDs ou a conversão de arquivos do LibreOffice. O Google™ também tem um mecanismo de pesquisa específico do Linux em `http://www.google.com/linux` que lhe pode ser útil.

Problemas comuns e suas soluções 31

Este capítulo descreve uma gama de problemas em potencial e suas soluções. Mesmo se a sua situação não esteja listada aqui com precisão, poderá haver alguma semelhante que ofereça dicas para a solução do seu problema.

31.1 Localizando e reunindo informações

O Linux reporta os dados de forma bastante detalhada. Há vários lugares para você pesquisar caso tenha problemas com seu sistema, sendo que a maioria é padrão para sistemas Linux em geral, e alguns relevantes aos sistemas SUSE Linux Enterprise Desktop. É possível ver a maioria dos arquivos de registro com o YaST (*Diversos* > *Registro de Inicialização*).

O YaST permite coletar todas as informações do sistema necessárias à equipe de suporte. Use *Outros* > *Suporte* e selecione a categoria do problema. Quando todas as informações forem reunidas, anexe-as à sua solicitação de suporte.

Veja a seguir uma lista dos arquivos de registro verificados com mais frequência com a descrição de seus objetivos principais. Os caminhos contendo ~ referem-se ao diretório pessoal do usuário atual.

Tabela 31.1 Arquivos de registro

Arquivo de registro	Descrição
`~/.xsession-errors`	Mensagens de aplicativos de área de trabalho atualmente em execução.
`/var/log/apparmor/`	Arquivos de registro do AppArmor, consulte a Part “Confining Privileges with AppArmor” (↑*Security Guide*) para obter informações detalhadas.
`/var/log/audit/audit.log`	Arquivo de registro do Audit para monitorar qualquer acesso a arquivos, diretórios ou recursos do seu sistema, bem como rastrear as chamadas do sistema.
`/var/log/boot.msg`	Mensagens do kernel reportadas durante o processo de boot.
`/var/log/mail.*`	Mensagens do sistema de correio.
`/var/log/messages`	Mensagens ininterruptas do kernel e do daemon de registro do sistema (durante a execução).
`/var/log/NetworkManager`	Arquivo de registro do NetworkManager para coleta de problemas de conectividade da rede
`/var/log/samba/`	Diretório contendo mensagens do registro de cliente e servidor do Samba.
`/var/log/SaX.log`	Mensagens de hardware do sistema KVM e da tela do SaX.
`/var/log/warn`	Todas as mensagens do kernel e do daemon do registro do sistema com o nível “warning” ou superior.

Arquivo de registro	Descrição
`/var/log/wtmp`	Arquivo binário contendo registros de login de usuário para a sessão da máquina atual. Exiba-o com `last`.
`/var/log/Xorg.*.log`	Vários registros de inicialização e tempo de execução do sistema X Window. São úteis para depurar inicializações malsucedidas do X.
`/var/log/YaST2/`	Diretório contendo ações do YaST e seus resultados.
`/var/log/zypper.log`	Arquivo de registro do zypper.

Além dos arquivos de registro, a sua máquina também lhe fornece informações sobre o sistema em execução. Consulte a Tabela 31.2: Informações do sistema no sistema de arquivos `/proc`.

Tabela 31.2 *Informações do sistema no sistema de arquivos /proc*

Arquivo	Descrição
`/proc/cpuinfo`	Contém informações do processador, incluindo o seu tipo, marca, modelo e desempenho.
`/proc/dma`	Mostra quais canais DMA estão sendo usados no momento.
`/proc/interrupts`	Mostra quais interrupções estão em uso e quantas de cada foram usadas.
`/proc/iomem`	Exibe o status da memória de E/S (entrada/saída).
`/proc/ioports`	Mostra quais portas de E/S estão em uso no momento.

Arquivo	Descrição
/proc/meminfo	Exibe o status da memória.
/proc/modules	Exibe os módulos individuais.
/proc/mounts	Exibe os dispositivos montados no momento.
/proc/partitions	Mostra o particionamento de todos os discos rígidos.
/proc/version	Exibe a versão atual do Linux.

Além do sistema de arquivos `/proc`, o kernel do Linux exporta informações com o módulo `sysfs`, um sistema de arquivos na memória. Esse módulo representa objetos Kernel, seus atributos e relacionamentos. Para obter mais informações sobre o `sysfs`, consulte o contexto de udev no Capítulo 16, *Gerenciamento dinâmico de dispositivos do Kernel com* `udev` (p 209). A Tabela 31.3 contém uma visão geral dos diretórios mais comuns em `/sys`.

Tabela 31.3 *Informações do sistema no sistema de arquivos /sys*

Arquivo	Descrição
/sys/block	Contém subdiretórios para cada dispositivo de bloco descoberto no sistema. Geralmente, esses dispositivos são de tipo de disco.
/sys/bus	Contém subdiretórios para cada tipo de barramento físico.
/sys/class	Contém subdiretórios agrupados como tipos funcionais de dispositivos (como gráficos, de rede, de impressora etc.)

Arquivo	Descrição
`/sys/device`	Contém a hierarquia global de dispositivos.

O Linux vem com várias ferramentas para monitoramento e análise do sistema. Consulte o Chapter 2, *System Monitoring Utilities* (↑*System Analysis and Tuning Guide*) para obter uma seleção das mais importantes usadas em diagnósticos de sistema.

Cada um dos seguintes cenários começa com um cabeçalho que descreve o problema, seguido de um ou dois parágrafos apresentando sugestões para solução, referências disponíveis para consultar soluções mais detalhadas e referências cruzadas para outros cenários relacionados.

31.2 Problemas de instalação

Problemas de instalação são situações que ocorrem quando a máquina falha na instalação. Ela pode falhar inteiramente ou talvez não consiga iniciar o instalador gráfico. Esta seção destaca alguns dos problemas típicos que você pode encontrar e oferece soluções ou alternativas possíveis para esses tipos de situações.

31.2.1 Verificação de mídia

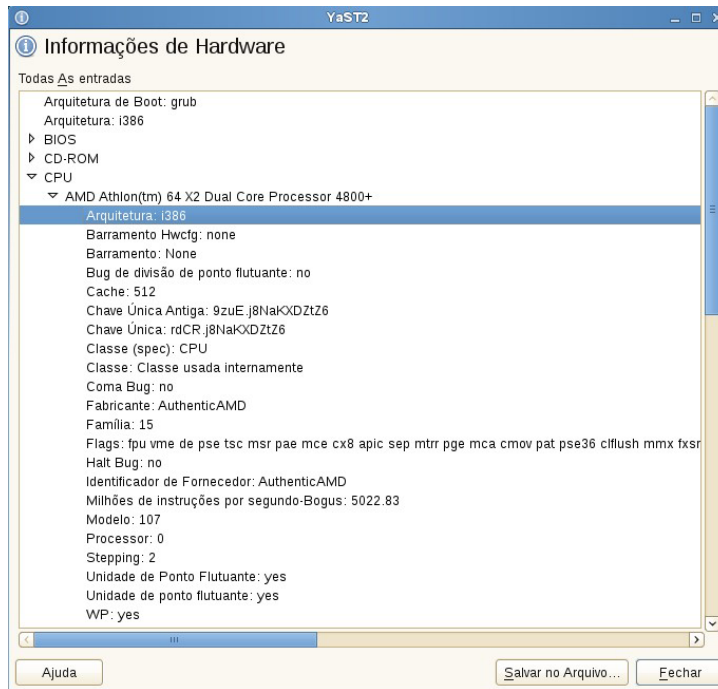
Se você tiver qualquer problema ao usar a mídia de instalação do SUSE Linux Enterprise Desktop, verifique a integridade da mídia em *Software* > *Verificação de Mídia*. Problemas de mídia são mais prováveis com a mídia que você mesmo gravou. Para verificar o meio do SUSE Linux Enterprise Desktop, insira-o na unidade e clique em *Iniciar Verificação* na tela *Verificação de Mídia* do YaST. Isso pode levar alguns minutos. Se forem detectados erros, não use esta mídia para instalação.

Figura 31.1 Verificação de mídia

31.2.2 Informações sobre hardware

Exiba hardware detectado e dados técnicos usando *Hardware* > *Informações de Hardware*. Clique em qualquer nó da árvore para obter mais informações sobre um dispositivo. Este módulo é especialmente útil quando você deseja enviar uma solicitação de suporte para a qual precisa de informações sobre o hardware.

Grave as informações de hardware exibidas em um arquivo clicando em *Salvar no Arquivo*. Selecione o nome de arquivo e diretório desejados e clique em *Salvar* para criar o arquivo.

Figura 31.2 *Exibindo informações sobre hardware*

31.2.3 Nenhuma unidade de DVD inicializável disponível

Se o seu computador não contém uma unidade de DVD-ROM inicializável ou se a que você tem não é suportada pelo Linux, há várias opções para instalar sua máquina sem uma unidade de DVD interna:

Inicializando de um disquete
: Crie um disquete de boot e inicialize por ele em vez de inicializar pelo DVD.

Usando um dispositivo de inicialização externo
: Se for suportado pelo BIOS e pelo kernel de instalação, inicialize pelas unidades de DVD externas.

Inicialização de rede via PXE
: Se uma máquina não tiver uma unidade de DVD, mas oferecer uma conexão de ethernet funcional, execute uma instalação completamente baseada em rede. Consulte a Section “Remote Installation via VNC—PXE Boot and Wake on LAN” (Chapter 11, *Remote Installation*, ↑*Deployment Guide*) e a Section “Remote Installation via SSH—PXE Boot and Wake on LAN” (Chapter 11, *Remote Installation*, ↑*Deployment Guide*) para obter os detalhes.

31.2.3.1 Inicializando de um disquete (SYSLINUX)

Em alguns computadores mais antigos, não há unidade de DVD inicializável disponível, mas há uma unidade de disquete. Para instalar em tal sistema, crie discos de inicialização e inicialize seu sistema com eles.

Os discos de boot incluem o carregador denominado SYSLINUX e o programa linuxrc. O SYSLINUX permite a seleção de um kernel durante o procedimento de inicialização e a especificação de quaisquer parâmetros necessários para o hardware usado. O programa linuxrc suporta o carregamento de módulos de kernel para o seu hardware e inicia subsequentemente a instalação.

Quando a inicialização é feita de um disquete de inicialização, o procedimento é iniciado pelo carregador de boot do SYSLINUX (pacote `syslinux`). Quando o sistema é inicializado, o SYSLINUX executa uma detecção mínima de hardware que consiste principalmente nas seguintes etapas:

1. O programa verifica se o BIOS fornece suporte de framebuffer compatível com VESA 2.0 e se inicializa o kernel de acordo.

2. Os dados do monitor (informações de DDC) são lidos.

3. O primeiro bloco do primeiro disco rígido (MBR) é lido para mapear IDs de BIOS para nomes de dispositivos do Linux durante a configuração do carregador de boot.

O programa tenta ler o bloco através das funções lba32 do BIOS para determinar se o BIOS suporta essas funções.

Se você mantiver Shift pressionado quando o SYSLINUX iniciar, todas essas etapas podem ser ignoradas. Para fins de solução de problemas, insira a linha

```
verbose 1
```

no `syslinux.cfg` para o carregador de boot exibir qual ação está sendo executada.

Se a máquina não inicializar do disquete, você talvez precise mudar a sequência de inicialização no BIOS para `A,C,CDROM`.

31.2.3.2 Dispositivos de inicialização externos

O Linux suporta a maioria das unidades de DVD existentes. Mesmo se o sistema não tiver uma unidade de DVD nem de disquete, ainda será possível usar uma unidade de DVD externa (conectada por USB, FireWire ou SCSI) para inicializar o sistema. Isso depende principalmente da interação entre o BIOS e o hardware usado. Algumas vezes uma atualização do BIOS pode ajudar se você tiver problemas.

31.2.4 Falha na inicialização da mídia de instalação

Um motivo possível para a máquina não inicializar a mídia de instalação é uma configuração incorreta de sequência de boot no BIOS. A sequência de boot do BIOS deve ter uma unidade de DVD definida como a primeira entrada de boot. De outra forma, a máquina tentaria inicializar de outro meio, normalmente o disco rígido. Diretrizes para mudar a sequência de boot do BIOS encontram-se na documentação fornecida com a placa-mãe ou nos parágrafos seguintes.

O BIOS é o software que habilita as funções mais básicas de um computador. Fabricantes de placas-mãe fornecem um BIOS especificamente fabricado para o hardware. Normalmente, a configuração do BIOS só pode ser acessada em um momento específico: quando a máquina está inicializando. Durante a fase de inicialização, a máquina executa vários testes de diagnóstico de hardware. Um deles é uma verificação de memória, indicado por um contador de memória. Quando o contador aparecer, procure uma linha, geralmente abaixo dele ou em algum local na parte inferior, mencionando a tecla a ser

pressionada para acessar a configuração do BIOS. Geralmente, a tecla a ser pressionada é Del, F1 ou Esc. Pressione esta tecla até que a tela de configuração do BIOS seja exibida.

Procedimento 31.1 *Mudando a sequência de inicialização do BIOS*

1. Digite o BIOS usando a tecla apropriada conforme anunciada pelas rotinas de inicialização e espere até que a tela do BIOS seja exibida.

2. Para mudar a sequência de inicialização em um AWARD BIOS, procure a entrada *BIOS FEATURES SETUP*. Outros fabricantes talvez tenham um nome diferente para isso, como *ADVANCED CMOS SETUP*. Quando encontrar a entrada, selecione-a e confirme com Enter.

3. Na tela exibida, procure uma subentrada denominada *BOOT SEQUENCE* ou *BOOT ORDER*. A sequência de boot é algo do tipo `C,A` ou `A,C`. Nesse caso, a máquina primeiro pesquisa o disco rígido (C) e, em seguida, o disquete (A) para encontrar um meio inicializável. Modifique as configurações pressionando PgUp ou PgDown até que a sequência seja `A,CDROM,C`.

4. Saia da tela de configuração do BIOS pressionando Esc. Para gravar as mudanças, selecione *SAVE & EXIT SETUP* ou pressione F10. Para confirmar que as configurações devem ser gravadas, pressione Y.

Procedimento 31.2 *Mudando a sequência de inicialização em um SCSI BIOS (Adaptador de Host Adaptec)*

1. Abra a configuração pressionando Ctrl + A.

2. Selecione *Utilitários de Disco*. Os componentes de hardware conectados agora são exibidos.

   Anote o ID do SCSI da sua unidade de DVD.

3. Saia do menu com Esc.

4. Abra *Definir Configurações do Adaptador*. Em *Opções Adicionais*, selecione *Opções do Dispositivo de Inicialização* e pressione Enter.

5. Digite o ID da unidade de DVD e pressione Enter novamente.

6. Pressione Esc duas vezes para retornar à tela de inicialização do BIOS do SCSI.

7 Saia dessa tela e confirme com *Sim* para inicializar o computador.

Independentemente do idioma e do layout do teclado que a instalação final usará, a maioria das configurações de BIOS usa o layout de teclado dos EUA, conforme mostrado na figura a seguir:

Figura 31.3 *Layout do teclado dos EUA*

31.2.5 Falha na inicialização

Alguns tipos de hardware, principalmente os muito antigos ou muito recentes, falham na instalação. Em muitos casos, isso pode ocorrer devido à ausência de suporte para esse tipo de hardware no kernel de instalação ou devido a alguma funcionalidade incluída nesse kernel, como a ACPI, que ainda causa problemas em alguns hardwares.

Se o seu sistema falhar na instalação usando o modo de *instalação* padrão da primeira tela de boot da instalação, tente o seguinte:

1 Com o DVD ainda na unidade, reinicialize a máquina com Ctrl + Alt + Del ou usando o botão de reinicialização do hardware.

2 Quando a tela de boot for exibida, pressione F5, use as teclas de seta do teclado para navegar até *Sem ACPI* e pressione Enter para iniciar o processo de boot e instalação. Essa opção desabilita o suporte para as técnicas de gerenciamento de energia da ACPI.

3 Prossiga com a instalação conforme descrito no Chapter 3, *Installation with YaST* (↑*Deployment Guide*).

Se isso falhar, proceda como acima, mas escolha *Configurações Seguras*. Essa opção desabilita o suporte de ACPI e DMA. A maioria dos hardwares inicializará com essa opção.

Se ambas as opções falharem, use o prompt das opções de boot para transmitir quaisquer parâmetros adicionais necessários para suportar esse tipo de hardware no kernel de instalação. Para obter mais informações sobre os parâmetros disponíveis como opções de boot, consulte a documentação do kernel localizada em `/usr/src/linux/Documentation/kernel-parameters.txt`.

DICA: obtendo documentação do kernel

Instale o pacote `kernel-source` para exibir a documentação do kernel.

Há vários outros parâmetros de kernel relacionados à ACPI que podem ser digitados no prompt de inicialização antes da inicialização para a instalação:

`acpi=off`
: Esse parâmetro desabilita o subsistema completo da ACPI no seu computador. Isso poderá ser útil se o computador não puder lidar com a ACPI de modo algum ou se você achar que a ACPI no computador causa problemas.

`acpi=force`
: Sempre habilite a ACPI mesmo que o computador tenha um BIOS antigo anterior ao ano 2000. Esse parâmetro também habilitará a ACPI se ele estiver definido além de `acpi=off`.

`acpi=noirq`
: Não use a ACPI para roteamento de IRQ.

`acpi=ht`
: Execute somente ACPI o suficiente para habilitar hyper-threading.

`acpi=strict`
: Tenha menos tolerância com plataformas que não sejam estritamente compatíveis com a especificação ACPI.

`pci=noacpi`
: Desabilita o roteamento de IRQ de PCI do novo sistema da ACPI.

`pnpacpi=off`
: Essa opção serve para problemas de porta serial ou paralela quando a configuração do BIOS contiver interrupções ou portas incorretas.

`notsc`
: Desabilita o contador da marcação de horário. Essa opção pode ser usada para solucionar problemas de tempo nos seus sistemas. Trata-se de um recurso recente, por isso, se você perceber regressões na sua máquina, especialmente relativas a horário ou mesmo um travamento total, vale a pena tentar essa opção.

`nohz=off`
: Desabilita o recurso nohz. Se a sua máquina trava, essa opção pode ajudar. Caso contrário, ela não tem utilidade.

Após determinar a combinação correta de parâmetros, o YaST os grava automaticamente na configuração do carregador de boot para verificar se o sistema inicializará de forma correta na próxima vez.

Se erros inexplicáveis ocorrerem quando o kernel estiver carregado ou durante a instalação, selecione *Teste de Memória* no menu de inicialização para verificar a memória. Se *Teste de Memória* retornar um erro, geralmente será um erro de hardware.

31.2.6 Falha na inicialização do instalador gráfico

Depois que você insere o meio na unidade e reinicializa a máquina, a tela de instalação é exibida, mas depois que a opção *Instalação* é selecionada, o instalador gráfico não inicializa.

Há várias maneiras de lidar com essa situação:

- Tente selecionar outra resolução de tela para as caixas de diálogo de instalação.
- Selecione *Modo de Texto* para a instalação.
- Faça uma instalação remota através de VNC usando o instalador gráfico.

Procedimento 31.3 *Mudar a resolução de tela para instalação*

1 Inicialize para a instalação.

2 Pressione F3 para abrir um menu do qual selecionar uma resolução mais baixa para fins de instalação.

3 Selecione *Instalação* e prossiga com a instalação conforme descrito no Chapter 3, *Installation with YaST* (↑*Deployment Guide*).

Procedimento 31.4 *Instalação em modo de texto*

1 Inicialize para a instalação.

2 Pressione F3 e selecione *Modo de Texto*.

3 Selecione *Instalação* e prossiga com a instalação conforme descrito no Chapter 3, *Installation with YaST* (↑*Deployment Guide*).

Procedimento 31.5 *Instalação VNC*

1 Inicialize para a instalação.

2 Insira o texto a seguir no prompt de opções de boot:

```
vnc=1 vncpassword=some_password
```

Substitua *senha* pela senha a ser usada para a instalação do VNC.

3 Selecione *Instalação* e pressione Enter para iniciar a instalação.

Em vez de iniciar com a rotina de instalação gráfica, o sistema continua em execução no modo de texto, depois trava, exibindo uma mensagem que contém o endereço IP e o número de porta com que o instalador pode ser acessado por uma interface de browser ou um aplicativo viewer do VNC.

4 Se estiver usando um browser para acessar o instalador, inicie o browser e digite as informações de endereço fornecidas pelas rotinas de instalação na futura máquina do SUSE Linux Enterprise Desktop e pressione Enter:

```
http://ip_address_of_machine:5801
```

Uma caixa de diálogo é aberta na janela do browser solicitando a senha VNC. Insira-a e continue com a instalação conforme descrito no Chapter 3, *Installation with YaST* (↑*Deployment Guide*).

> **IMPORTANTE**
>
> A instalação através de VNC funciona com qualquer navegador em qualquer sistema operacional, desde que o suporte Java esteja habilitado.

Forneça o endereço IP e a senha do seu viewer do VNC quando solicitado. Uma janela é aberta, exibindo as caixas de diálogo de instalação. Prossiga com a instalação como de costume.

31.2.7 Apenas a tela de boot simples é aberta

Você inseriu o meio na unidade, as rotinas do BIOS foram encerradas, mas o sistema não inicia com a tela de boot gráfica. Em vez disso, ele inicia uma interface baseada em texto bastante simples. Isso pode acontecer em qualquer máquina que não forneça memória gráfica suficiente para renderizar uma tela de boot gráfica.

Embora a tela de boot de texto tenha aparência simples, ela fornece praticamente a mesma funcionalidade que a gráfica:

Opções de Boot
: Diferentemente da interface gráfica, as diversas opções de boot não podem ser selecionadas usando as teclas de cursor do teclado. O menu de inicialização da tela de boot em modo de texto oferece algumas palavras-chave no prompt de inicialização. Essas palavras-chave são mapeadas para as opções oferecidas na versão gráfica. Insira sua escolha e pressione Enter para iniciar o processo de boot.

Opções de Boot Personalizadas
: Após selecionar uma opção de boot, insira a palavra-chave apropriada no prompt de boot ou insira algumas opções de boot personalizadas conforme descrito na Seção 31.2.5, “Falha na inicialização” (p 445). Para iniciar o processo de instalação, pressione Enter.

Resoluções de tela
: Use as teclas F para determinar a resolução de tela para a instalação. Se você precisa inicializar no modo de texto, escolha F3.

31.3 Problemas de boot

Problemas de boot são situações em que o sistema não inicializa de forma adequada (não inicializa no nível de execução e na tela de login esperados).

31.3.1 Falha ao carregar o carregador de boot GRUB

Se o hardware estiver funcionando de forma adequada, é possível que o carregador de boot esteja corrompido e que o Linux não possa ser iniciado na máquina. Nesse caso, é necessário reinstalar o carregador de boot. Para reinstalar o carregador de boot, proceda da seguinte maneira:

1. Insira a mídia de instalação na unidade.

2. Reinicialize a máquina.

3. Selecione *Instalação* no menu de inicialização.

4. Selecione um idioma.

5. Aceite o contrato de licença.

6. Na tela *Modo de Instalação*, selecione *Reparar o Sistema Instalado*.

7. Quando estiver no módulo YaST Reparo do Sistema, selecione *Ferramentas Especialista* e selecione *Instalar Novo Bootloader*.

8. Restaure as configurações originais e reinstale o carregador de boot.

9. Saia de YaST Reparo do Sistema e reinicialize o sistema.

Outros motivos para a máquina não inicializar podem estar relacionadas ao BIOS:

Configurações do BIOS
: Verifique o BIOS para obter referências para o disco rígido. O GRUB talvez não seja iniciado se o próprio disco rígido não puder se encontrado com as configurações atuais do BIOS.

Ordem de inicialização do BIOS
: Verifique se a ordem de inicialização do sistema inclui o disco rígido. Se a opção do disco rígido não tiver sido habilitada, o sistema talvez seja instalado de forma adequada, mas não seja inicializado quando o acesso ao disco rígido for necessário.

31.3.2 Não é exibido nenhum prompt nem tela de login

Isso costuma ocorrer após uma falha de atualização do kernel e é conhecido como *pânico do kernel* devido ao tipo de erro do console do sistema que às vezes se verifica no estágio final do processo. Se a máquina realmente tiver sido reinicializada após uma atualização de software, o objetivo imediato é reinicializá-la usando a versão antiga e segura do kernel do Linux e os arquivos associados. Isso pode ser feito na tela do carregador de boot GRUB durante o processo de inicialização da seguinte forma:

1. Reinicialize o computador usando o botão de reinicialização ou desligue-o e ligue-o novamente.

2. Quando a tela de boot do GRUB for exibida, selecione *Linux--Failsafe* e pressione Enter. A máquina será inicializada com a versão anterior do kernel e seus arquivos associados.

3. Após a conclusão do processo de boot, remova o kernel recém-instalado e, se necessário, modifique manualmente `/boot/grub/menu.lst` para tornar o kernel mais antigo a opção padrão. Para obter informações detalhadas sobre a sintaxe usada nesse arquivo de configuração, consulte o Capítulo 12, *O carregador de boot GRUB* (p 143).

   A atualização desse arquivo pode não ser necessária porque as ferramentas automatizadas de atualização geralmente o modificam durante o processo de rollback.

4. Reinicializar.

Se isso não resolver o problema porque a opção *Linux--Failsafe* não inicia o computador como deveria, inicialize-o usando a mídia de instalação. Após a inicialização da máquina, prossiga com o Passo 3 (p 451).

31.3.3 Não há login gráfico

Se a máquina ligar, mas não inicializar no gerenciador de login gráfico, evite problemas com a escolha do nível de execução padrão ou a configuração do sistema X Window. Para verificar a configuração do nível de execução, efetue login como o usuário `root` e verifique se a máquina está configurada para inicializar no nível de execução 5 (área de trabalho gráfica). Uma maneira rápida de verificar isso é examinar o conteúdo de `/etc/inittab`, da seguinte maneira:

```
tux@mercury:~> grep "id:" /etc/inittab
id:5:initdefault:
```

A linha retornada indica que o nível de execução padrão da máquina (`initdefault`) está definido como `5` e que ela deve inicializar na área de trabalho gráfica. Se o nível de execução estiver definido como qualquer outro número, use o módulo YaST Editor de Níveis de Execução para defini-lo como `5`.

IMPORTANTE

Não edite a configuração do nível de execução manualmente. Caso contrário, o SuSEconfig (executado pelo YaST) sobrescreverá essas mudanças na próxima execução. Se você precisa fazer mudanças manuais aqui, desabilite mudanças futuras do SuSEconfig definindo *`CHECK_INITTAB`* em `/etc/sysconfig/suseconfig` como `no`.

Se o nível de execução estiver definido como `5`, provavelmente a sua área de trabalho ou o software X Window está mal configurado ou corrompido. Examine os arquivos de registro em `/var/log/Xorg.*.log` para obter mensagens detalhadas do servidor X enquanto ele tenta iniciar. Se a área de trabalho falhar durante a inicialização, talvez ela registre mensagens de erro em `/var/log/messages`. Se essas mensagens de erro sugerirem um problema de configuração no servidor X, tente corrigi-lo. Se o sistema gráfico ainda não aparecer, reinstale a área de trabalho gráfica.

DICA: iniciando o sistema X Window manualmente

Um teste rápido: o comando `startx` deverá forçar o sistema X Window a iniciar com os padrões configurados se o usuário estiver logado no console. Se isso não funcionar, ele deve registrar erros no console.

31.4 Problemas de login

Problemas de login são aqueles em que sua máquina, de fato, inicializa na tela de boas-vindas ou no prompt de login, como esperado, mas recusa-se a aceitar o nome de usuário e a senha ou aceita-os mas não se comporta de forma adequada (não inicia a área de trabalho gráfica, produz erros, passa para uma linha de comando, entre outros).

31.4.1 Falha nas combinações de nome de usuário e senha válidas

Isso geralmente ocorre quando o sistema está configurado para usar autenticação de rede ou serviços de diretório e, por alguma razão, não é capaz de recuperar resultados de seus servidores configurados. O usuário `root`, como o único usuário local, é o único que ainda pode efetuar login nessas máquinas. A seguir estão alguns motivos comuns para uma máquina parecer funcional, mas não conseguir processar logins corretamente:

- A rede não está funcionando. Para obter mais instruções sobre isso, consulte a Seção 31.5, “Problemas de rede” (p 461).

- O DNS não está funcionando no momento (o que impede o GNOME ou o KDE de trabalhar e o sistema de efetuar solicitações válidas a servidores seguros). Uma indicação de que esse é o caso é que a máquina leva muito tempo para responder a qualquer ação. Há mais informações a respeito desse tópico na Seção 31.5, “Problemas de rede” (p 461).

- Se o sistema estiver configurado para usar Kerberos, o horário local do sistema poderá ter ultrapassado a variação aceita com o horário do servidor Kerberos (geralmente 300 segundos). Se o NTP (protocolo de horário de rede) não estiver funcionando de forma adequada ou os servidores NTP locais não estiverem funcionando, a

autenticação do Kerberos não funcionará pois depende da sincronização comum do relógio na rede.

- A configuração de autenticação do sistema está definida incorretamente. Verifique se há erros de digitação ou ordem incorreta de diretivas nos arquivos de configuração PAM envolvidos. Para obter informações adicionais sobre o PAM e a sintaxe dos arquivos de configuração envolvidos, consulte o Chapter 2, *Authentication with PAM* (↑*Security Guide*).

- A partição pessoal está criptografada. Há mais informações a respeito desse tópico na Seção 31.4.3, “Falha de login na partição pessoal criptografada” (p 458).

Em todos os casos que não envolvem problemas de rede externos, a solução é reinicializar o sistema em um modo de usuário único e reparar a configuração antes de inicializar novamente no modo de operação e tentar efetuar login novamente. Para inicializar no modo de usuário único:

1. Reinicialize o sistema. A tela de boot é exibida e apresenta um prompt.

2. Insira `1` no prompt de inicialização para fazer o sistema inicializar no modo de usuário único.

3. Insira o nome de usuário e a senha para `root`.

4. Faça as mudanças necessárias.

5. Inicialize no modo de rede e multiusuário total digitando `telinit 5` na linha de comando.

31.4.2 Nome de usuário e senha válidos não foram aceitos

Esse é o um dos problemas mais comuns que os usuários podem encontrar, pois há vários motivos pelos quais isso pode ocorrer. Dependendo de você usar gerenciamento e autenticação de usuário local ou autenticação em rede, as falhas de login ocorrem por motivos diferentes.

O gerenciamento de usuário local pode falhar pelos seguintes motivos:

- O usuário pode ter digitado a senha errada.
- O diretório pessoal do usuário que contém arquivos de configuração da área de trabalho está corrompido ou protegido contra gravação.
- Talvez haja problemas com o sistema X Window ao autenticar esse usuário específico, especialmente se o diretório pessoal do usuário tiver sido usado com outra distribuição do Linux antes da instalação da atual.

Para encontrar o motivo de uma falha de login local, proceda da seguinte maneira:

1 Verifique se o usuário memorizou a senha corretamente antes de começar a depurar todo o mecanismo de autenticação. Se o usuário não se lembrar da senha corretamente, use o módulo Gerenciamento de Usuário do YaST para mudar a senha dele. Fique atento à tecla Caps Lock e libere-a, se necessário.

2 Efetue login como `root` e, em `/var/log/messages`, verifique se há mensagens de erro do processo de login e do PAM.

3 Tente efetuar login de um console (usando Ctrl + Alt + F1). Se esse procedimento for bem-sucedido, não será responsabilidade do PAM, pois é possível autenticar o usuário nessa máquina. Tente localizar quaisquer problemas com o sistema X Window ou a área de trabalho (GNOME ou KDE). Para obter mais informações, consulte a Seção 31.4.4, “Login bem-sucedido, mas há falha na área de trabalho do GNOME” (p 458) e a Seção 31.4.5, “Login bem-sucedido mas há falha na área de trabalho do KDE” (p 459).

4 Se o diretório pessoal do usuário foi usado com outra distribuição Linux, remova o arquivo `Xauthority` no diretório do usuário. Use um login de console por meio de Ctrl + Alt + F1 e execute o comando `rm .Xauthority` como esse usuário. Isso deve eliminar problemas de autenticação X para o usuário. Tente o login gráfico novamente.

5 Se o login gráfico ainda falhar, efetue um login de console com Ctrl + Alt + F1. Tente iniciar uma sessão X em outra tela — a primeira (`:0`) já está em uso:

```
startx -- :1
```

Isso deve exibir uma tela gráfica e a sua área de trabalho. Se não, verifique os arquivos de registro do sistema X Window (`/var/log/Xorg.`*`número_de_exibição`*`.log`) ou o arquivo de registro para seus aplicativos de área de trabalho (

`.xsession-errors` no diretório pessoal do usuário) em busca de quaisquer irregularidades.

6. Se a área de trabalho não puder iniciar devido a arquivos de configuração corruptos, continue com a Seção 31.4.4, “Login bem-sucedido, mas há falha na área de trabalho do GNOME” (p 458) ou a Seção 31.4.5, “Login bem-sucedido mas há falha na área de trabalho do KDE” (p 459).

Veja a seguir alguns motivos comuns pelos quais a autenticação em rede de um usuário específico pode falhar em uma máquina específica:

- O usuário pode ter digitado a senha errada.
- O nome de usuário existe nos arquivos de autenticação local da máquina e também é fornecido por um sistema de autenticação de rede, causando conflitos.
- O diretório pessoal existe mas está corrompido ou não disponível. Talvez ele esteja protegido contra gravação ou está em um servidor inacessível no momento.
- O usuário não tem permissão para efetuar login neste host específico no sistema de autenticação.
- A máquina mudou de nomes de host, por qualquer motivo, e o usuário não tem permissão para efetuar login no host.
- A máquina não pode acessar o servidor de diretório ou o servidor de autenticação que contém as informações do usuário.
- Talvez haja problemas com o sistema X Window ao autenticar esse usuário específico, especialmente se o diretório pessoal do usuário tiver sido usado com outra distribuição do Linux antes da instalação da atual.

Para localizar a causa das falhas de login com a autenticação de rede, proceda da seguinte maneira:

1. Verifique se o usuário memorizou a senha corretamente antes de começar a depurar todo o mecanismo de autenticação.

2. Determine o servidor de diretórios usado pela máquina para autenticação e verifique se ele está funcionando e se comunicando corretamente com as outras máquinas.

3. Determine se o nome e a senha do usuário funcionam em outras máquinas para verificar se os dados de autenticação existem e são distribuídos corretamente.

4. Verifique se outro usuário pode efetuar login na máquina com comportamento incorreto. Se outro usuário ou o usuário `root` puder efetuar login sem dificuldade, conecte-se e examine o arquivo `/var/log/messages`. Localize as marcações de horário que correspondem às tentativas de login e determine se o PAM produziu alguma mensagem de erro.

5. Tente efetuar login de um console (usando Ctrl + Alt + F1). Se der certo, o problema não é do PAM ou do servidor de diretórios no qual o diretório pessoal do usuário está hospedado, pois é possível autenticar o usuário nessa máquina. Tente localizar quaisquer problemas com o sistema X Window ou a área de trabalho (GNOME ou KDE). Para obter mais informações, consulte a Seção 31.4.4, “Login bem-sucedido, mas há falha na área de trabalho do GNOME” (p 458) e a Seção 31.4.5, “Login bem-sucedido mas há falha na área de trabalho do KDE” (p 459).

6. Se o diretório pessoal do usuário foi usado com outra distribuição Linux, remova o arquivo `Xauthority` no diretório do usuário. Use um login de console por meio de Ctrl + Alt + F1 e execute o comando `rm .Xauthority` como esse usuário. Isso deve eliminar problemas de autenticação X para o usuário. Tente o login gráfico novamente.

7. Se o login gráfico ainda falhar, efetue um login de console com Ctrl + Alt + F1. Tente iniciar uma sessão X em outra tela — a primeira (`:0`) já está em uso:

   ```
   startx -- :1
   ```

   Isso deve exibir uma tela gráfica e a sua área de trabalho. Se não, verifique os arquivos de registro do sistema X Window (`/var/log/Xorg.`*`número_de_exibição`*`.log`) ou o arquivo de registro para seus aplicativos de área de trabalho (`.xsession-errors` no diretório pessoal do usuário) em busca de quaisquer irregularidades.

8. Se a área de trabalho não puder iniciar devido a arquivos de configuração corruptos, continue com a Seção 31.4.4, “Login bem-sucedido, mas há falha na área de trabalho do GNOME” (p 458) ou a Seção 31.4.5, “Login bem-sucedido mas há falha na área de trabalho do KDE” (p 459).

31.4.3 Falha de login na partição pessoal criptografada

Recomenda-se o uso de uma partição pessoal criptografada para laptops. Se você não puder efetuar login no seu laptop, o motivo geralmente é simples: a sua partição pode não estar desbloqueada.

No momento da inicialização, você precisa digitar a frase secreta para desbloquear a sua partição criptografada. Se você não a digitar, o processo de boot continuará, deixando a partição bloqueada.

Para desbloquear a partição criptografada, faça o seguinte:

1 Passe para o console de texto com Ctrl + Alt + F1.

2 Torne-se `root`.

3 Reinicie o processo de desbloqueio novamente com:

```
/etc/init.d/boot.crypto restart
```

4 Digite sua frase secreta para desbloquear a partição criptografada.

5 Saia do console de texto e volte para a tela de login com Alt + F7.

6 Efetue login como de costume.

31.4.4 Login bem-sucedido, mas há falha na área de trabalho do GNOME

Se esse for o caso, provavelmente os seus arquivos de configuração do GNOME se corromperam. Alguns sintomas podem incluir falha de funcionamento do teclado, a geometria da tela distorcida ou até mesmo a tela exibida como um campo cinza vazio. A distinção importante é que se outro usuário efetuar login, a máquina funcionará normalmente. Provavelmente o problema possa ser corrigido rapidamente com a transferência do diretório de configuração do GNOME do usuário para um novo local,

o que faz a área de trabalho do GNOME inicializar um novo. Embora o usuário seja forçado a reconfigurar o GNOME, nenhum dado é perdido.

1. Alterne para um console de texto pressionando Ctrl + Alt + F1.

2. Efetue login com o seu nome de usuário.

3. Mova os diretórios de configuração do GNOME do usuário para um local temporário:

```
mv .gconf  .gconf-ORIG-RECOVER
mv .gnome2 .gnome2-ORIG-RECOVER
```

4. Efetue logout.

5. Efetue login novamente, mas não execute nenhum aplicativo.

6. Recupere seus dados individuais de configuração de aplicativo (inclusive os dados de cliente de e-mail do Evolution) copiando o diretório `~/gconf-ORIG-RECOVER/apps/` de volta para o novo diretório `~/.gconf` da seguinte maneira:

```
cp -a .gconf-ORIG-RECOVER/apps .gconf/
```

   Se isso causar os problemas de login, tente recuperar somente os dados de aplicativo críticos e reconfigure o restante dos aplicativos.

31.4.5 Login bem-sucedido mas há falha na área de trabalho do KDE

Há vários motivos pelos quais uma área de trabalho do KDE não permitiria que usuários efetuassem login. Dados de cache corrompidos podem causar problemas de login e arquivos de configuração de área de trabalho do KDE corrompidos.

Dados de cache são usados na inicialização da área de trabalho para aumentar o desempenho. Se os dados estiverem corrompidos, a inicialização será mais lenta ou falhará inteiramente. Removê-los força as rotinas de inicialização da área de trabalho a iniciarem desde o começo. Isso leva mais tempo do que uma inicialização normal, mas os dados estarão intactos depois disso e o usuário poderá efetuar login.

Para remover os arquivos de cache da área de trabalho do KDE, emita o seguinte comando como `root`:

```
rm -rf /tmp/kde-user /tmp/ksocket-user
```

Substitua *usuário* pelo seu nome de usuário. A remoção desses dois diretórios remove somente os arquivos de cache corrompidos. Nenhum dado real é danificado por esse procedimento.

Arquivos de configuração de área de trabalho corrompidos sempre podem ser substituídos pelos arquivos de configuração inicial. Se você deseja recuperar os ajustes do usuário, copie-os cuidadosamente de volta do local temporário após a configuração ter sido restaurada usando os valores de configuração padrão.

Para substituir uma configuração de área de trabalho corrompida pelos valores de configuração inicial, proceda da seguinte maneira:

1. Alterne para um console de texto pressionando Ctrl + Alt + F1.

2. Efetue login com o seu nome de usuário.

3. Mova o diretório de configuração do KDE e os arquivos `.skel` para um local temporário:

   - Para o KDE3, use estes comandos:

     ```
     mv .kde  .kde-ORIG-RECOVER
     mv .skel .skel-ORIG-RECOVER
     ```

   - Para o KDE4, use estes comandos:

     ```
     mv .kde4  .kde4-ORIG-RECOVER
     mv .skel .skel-ORIG-RECOVER
     ```

4. Efetue logout.

5. Efetue login novamente.

6. Após a inicialização bem-sucedida da área de trabalho, copie a configuração do usuário de volta no local:

   ```
   cp -a KDEDIR/share .kde/share
   ```

   Substitua *KDEDIR* pelo diretório do Passo 3 (p 460).

IMPORTANTE

Se os ajustes do usuário causaram a falha no login e continuam a fazer isso, repita o procedimento como descrito acima, mas não copie o diretório `.kde/share`.

31.5 Problemas de rede

Quaisquer problemas do seu sistema podem estar relacionados à rede, mesmo que inicialmente não transmitam essa impressão. Por exemplo, o motivo para um sistema não permitir o login de usuários pode ser algum tipo de problema de rede. Esta seção apresenta uma lista de verificação simples que você pode aplicar para identificar a causa de qualquer problema de rede encontrado.

Procedimento 31.6 *Como identificar problemas de rede*

Ao verificar a conexão de rede da sua máquina, proceda da seguinte maneira:

1. Se você estiver usando uma conexão ethernet, verifique o hardware primeiro. Verifique se o cabo de rede está acoplado corretamente no computador e no roteador (ou hub etc.). As luzes de controle próximas ao seu conector ethernet devem estar ativas.

   Se a conexão falhar, verifique se o cabo de rede funciona com outra máquina. Se funcionar, a placa de rede será a causa da falha. Se houver hubs ou switches incluídos na configuração da sua rede, eles também podem estar com defeito.

2. Se estiver usando uma conexão sem fio, verifique se o link sem fio pode ser estabelecido por outras máquinas. Caso contrário, contate o administrador da rede wireless.

3. Após verificar sua conectividade de rede básica, tente descobrir qual serviço não está respondendo. Reúna as informações de endereço de todos os servidores de rede necessários na configuração. Procure-os no módulo YaST apropriado ou consulte o administrador de sistema. A lista a seguir fornece alguns dos servidores de rede típicos envolvidos em uma configuração junto com os sintomas de uma falha.

DNS (Serviço de Nomes)
: Um serviço de nomes inoperante ou defeituoso afeta a funcionalidade da rede de várias maneiras. Se a máquina local depender de quaisquer servidores de rede para autenticação e esses servidores não puderem ser encontrados devido a problemas de resolução de nomes, os usuários não serão capazes nem de efetuar login. As máquinas da rede gerenciadas por um servidor de nomes inoperante não seriam capazes de “ver” umas às outras e de se comunicarem.

NTP (Serviço de Horário)
: Um serviço NTP defeituoso ou totalmente inoperante pode afetar a funcionalidade do servidor X e a autenticação Kerberos.

NFS (Serviço de Arquivos)
: Se qualquer aplicativo precisar de dados armazenados em um diretório NFS montado, ele não conseguirá iniciar nem funcionar corretamente se esse serviço estiver inoperante ou mal configurado. No pior cenário possível, a configuração da área de trabalho pessoal de um usuário não será exibida se o seu diretório pessoal que contém os subdiretórios `.gconf` ou `.kde` não forem encontrados devido a falha do servidor NFS.

Samba (Serviço de Arquivos)
: Se qualquer aplicativo precisar de dados armazenados em um diretório de um servidor Samba defeituoso, ele não conseguirá iniciar ou funcionar corretamente.

NIS (Gerenciamento de Usuário)
: Se o sistema SUSE Linux Enterprise Desktop usar um servidor NIS defeituoso para fornecer os dados de usuários, os usuários não poderão efetuar login na máquina.

LDAP (Gerenciamento de Usuário)
: Se o sistema SUSE Linux Enterprise Desktop usar um servidor LDAP defeituoso para fornecer os dados de usuários, os usuários não poderão efetuar login na máquina.

Kerberos (Autenticação)
: A autenticação não funcionará e o login em qualquer máquina falhará.

CUPS (Impressão de Rede)
: Os usuários não conseguem imprimir.

4 Verifique se os servidores de rede estão em execução e se a configuração de rede permite estabelecer uma conexão:

IMPORTANTE

O procedimento de depuração descrito abaixo aplica-se somente a uma configuração simples de servidor/cliente de rede que não envolva roteamento interno. Supõe-se que o servidor e o cliente integrem a mesma sub-rede sem necessidade de roteamento adicional.

4a Use `ping` *`endereço IP`* `ou` *`nome_do_host`* (substitua *`nome_do_host`* pelo nome do host do servidor) para verificar se cada um deles está funcionando e respondendo à rede. Se esse comando for bem-sucedido, ele informará que o host que você estava procurando está em execução e o serviço de nomes da rede está configurado corretamente.

Se o ping falhar com `destination host unreachable`, o seu sistema ou o servidor desejado não está configurado de forma adequada ou está inoperante. Verifique se o sistema pode ser alcançado com `ping` *`endereço IP`* `ou` *`seu_nome_de_host`* em outra máquina. Se você obtiver êxito em acessar sua máquina de outra máquina, significará que o servidor não está sendo executado ou não está configurado corretamente.

Se o ping falhar com `unknown host`, significará que o serviço de nomes não está configurado corretamente ou o nome do host usado estava incorreto. Para obter mais verificações sobre esse assunto, consulte o Passo 4b (p 463). Se o ping ainda falhar, significará que a placa de rede não está configurada de forma correta ou o hardware de rede está defeituoso.

4b Use `host` *`nome_do_host`* para verificar se o nome do host do servidor ao qual você está tentando se conectar está convertido de forma adequada em um endereço IP e vice-versa. Se esse comando retornar o endereço IP do host, significará que o serviço de nomes está funcionando. Se houver falha nesse comando `host`, verifique todos os arquivos de configuração de rede relacionados à resolução de nomes e de endereços no seu host:

`/etc/resolv.conf`

Este arquivo é usado para controlar o domínio e o servidor de nomes que você está usando no momento. Ele pode ser modificado manualmente ou ajustado automaticamente pelo YaST ou DHCP. O ajuste automático é preferencial. Porém, verifique se o arquivo tem a estrutura a seguir e se todos os endereços de rede e nomes de domínio estão corretos:

```
search fully_qualified_domain_name
nameserver ipaddress_of_nameserver
```

Este arquivo pode conter mais de um endereço de servidor de nomes, mas pelo menos um deles deve estar correto para fornecer a resolução de nomes para o seu host. Se necessário, ajuste o arquivo usando o módulo Configurações de Rede do YaST (guia Nome de host/DNS).

Se a conexão de rede for gerenciada por DHCP, habilite o DHCP para mudar as informações de serviço de nomes e nome de host selecionando *Modificar Nome de Host via DHCP* e *Atualizar Servidor de Nomes e Lista de Pesquisa via DHCP* no módulo YaST DNS e Nome de Host.

`/etc/nsswitch.conf`

Este arquivo informa ao Linux onde procurar informações de serviço de nomes. Ele deve ter a seguinte aparência:

```
 ...
hosts: files dns
networks: files dns
...
```

A entrada `dns` é essencial. Ela informa ao Linux para usar um servidor de nomes externo. Normalmente, essas entradas são gerenciadas automaticamente pelo YaST, mas convém verificar.

Se todas as entradas relevantes no host estiverem corretas, deixe o seu administrador de sistema verificar a configuração do servidor DNS para obter as informações de zona corretas. Se você verificou se a configuração DNS do seu host e o servidor DNS estão corretos, continue verificando a configuração da rede e do dispositivo de rede.

4c Se o sistema não puder estabelecer uma conexão a um servidor de redes e você excluiu problemas de serviço de nomes da lista de possíveis responsáveis, verifique a configuração da placa de rede.

Use o comando `ifconfig` *`dispositivo_de_rede`* (executado como `root`) para verificar se este dispositivo foi configurado de forma adequada. Verifique se `inet address` e `Mask` estão configurados corretamente. Um erro no endereço IP ou um bit ausente na máscara de rede inutilizam a configuração de rede. Se necessário, execute essa verificação no servidor também.

4d Se o hardware de rede e o serviço de nomes estiverem configurados de forma adequada e em execução, mas algumas conexões de rede externas ainda tiverem longos tempos de espera ou falharem inteiramente, use `traceroute` *`nome_completo_do_domínio`* (executado como `root`) para controlar a rota de rede tomada pelas solicitações. Esse comando lista qualquer gateway (hop) que uma solicitação da sua máquina transmitir no caminho ao seu destino. Ele lista o tempo de resposta de cada hop e se esse hop é acessível. Use uma combinação de traceroute e ping para identificar o responsável e informar aos administradores.

Após identificar a causa do problema de rede, você poderá resolvê-lo (se o problema estiver na sua máquina) ou informar os administradores de sistema da rede sobre suas descobertas para que eles possam reconfigurar os serviços ou reparar os sistemas necessários.

31.5.1 Problemas no NetworkManager

Se você tiver problema com a conectividade da rede, restrinja-a conforme descrito no Procedimento 31.6, “Como identificar problemas de rede” (p 461). Se tudo indicar que a culpa é do NetworkManager, faça o seguinte para obter os registros com dicas sobre o motivo da falha do NetworkManager:

1. Abra um shell e efetue login como `root`.

2. Reinicie o NetworkManager:

   ```
   rcnetwork restart -o nm
   ```

3. Abra uma página da Web, por exemplo http://www.opensuse.org, como usuário normal para ver se você consegue se conectar.

4 Colete as informações sobre o estado do NetworkManager em `/var/log/NetworkManager`.

Para obter maiores informações sobre o NetworkManager, consulte o Capítulo 26, *Usando o NetworkManager* (p 379).

31.6 Problemas de dados

Problemas de dados ocorrem quando a máquina pode ou não inicializar corretamente, mas em ambos os casos, está claro que há dados corrompidos no sistema e que o sistema precisa ser recuperado. Essas situações exigem um backup dos seus dados críticos, permitindo que você recupere o estado anterior à falha do sistema. O SUSE Linux Enterprise Desktop oferece módulos do YaST dedicados para backup e restauração do sistema e um sistema de recuperação que pode ser usado para recuperar um sistema corrompido externamente.

31.6.1 Gerenciando imagens de partição

Às vezes é necessário fazer um backup de uma partição inteira ou até do disco rígido. O Linux possui a ferramenta `dd`, capaz de criar uma cópia exata do seu disco. Combinada ao `gzip`, faz você economizar espaço.

Procedimento 31.7 *Fazendo backup e restaurando discos rígidos*

1 Inicie um Shell como usuário `root`.

2 Selecione o seu dispositivo de origem. Normalmente, ele assemelha-se a `/dev/sda` (com a etiqueta *SOURCE*).

3 Indique onde deseja armazenar sua imagem (com a etiqueta *CAMINHO_BACKUP*). Esse local deverá ser diferente do dispositivo de origem. Em outras palavras: se você fizer backup de `/dev/sda`, seu arquivo de imagem poderá não ser armazenado em `/dev/sda`.

4 Execute os comandos para criar um arquivo de imagem compactado:

```
dd if=/dev/SOURCE | gzip > /BACKUP_PATH/image.gz
```

5 Recupere o disco rígido usando os seguintes comandos:

```
gzip -dc /BACKUP_PATH/image.gz | dd of=/dev/SOURCE
```

Se você precisar de apenas uma partição para o backup, substitua o marcador *SOURCE* pela sua respectiva partição. Nesse caso, o seu arquivo de imagem pode usar o mesmo disco rígido, só que em outra partição.

31.6.2 Fazendo backup de dados críticos

Backups de sistema podem ser facilmente gerenciados usando o módulo YaST Backup do Sistema:

1 Como `root`, inicie o YaST e selecione *Sistema* > *Backup do Sistema*.

2 Crie um perfil de backup com todos os detalhes necessários para o backup, o nome do arquivo, o escopo e o tipo de backup:

2a Selecione *Gerenciamento de Perfil* > *Adicionar*.

2b Especifique um nome para o arquivo.

2c Insira o caminho no local do backup se desejar manter um backup local. Para que seu backup seja arquivado em um servidor de rede (via NFS), insira o endereço IP ou o nome do servidor e o diretório que deve armazenar seu arquivo.

2d Determine o tipo de arquivo e clique em *Avançar*.

2e Determine as opções de backup a serem usadas, se os arquivos não pertencentes a algum pacote devem sofrer backup e se uma lista de arquivos deve ser exibida antes da criação do arquivo. Determine também se os arquivos mudados devem ser identificados usando o mecanismo MD5 demorado.

Use *Especialista* para inserir uma caixa de diálogo para o backup de áreas inteiras de disco rígido. Atualmente, essa opção aplica-se somente ao sistema de arquivos Ext2.

2f Por fim, defina as restrições de pesquisa para excluir da área de backup determinadas áreas do sistema que não precisam de backup, como arquivos

de bloqueio e de cache. Adicione, edite ou apague itens até que suas necessidades sejam atendidas e saia com *OK*.

3 Após terminar as configurações de perfil, você pode começar o backup imediatamente com *Criar Backup* ou configurar o backup automático. Também é possível criar outros perfis adaptados para várias outras finalidades.

Para configurar o backup automático de um determinado perfil, proceda da seguinte maneira:

1 Selecione *Backup Automático* no menu *Gerenciamento de Perfil*.

2 Selecione *Iniciar Backup Automaticamente*.

3 Determine a frequência de backup. Escolha *diariamente*, *semanalmente* ou *mensalmente*.

4 Determine o horário de início do backup. Essas configurações dependem da frequência de backup selecionada.

5 Decida se manterá backups antigos e quantos devem ser mantidos. Para receber uma mensagem de status gerada automaticamente do processo de backup, marque *Enviar Mensagem de Resumo ao Usuário root*.

6 Clique em *OK* para aplicar suas configurações e fazer com que o primeiro backup seja iniciado no horário especificado.

31.6.3 Restaurando um backup de sistema

Use o módulo YaST Restauração do Sistema para restaurar a configuração de sistema de um backup. Restaure todo o backup ou selecione componentes específicos que estavam corrompidos e precisam ser redefinidos ao estado antigo.

1 Inicie *YaST* > *Sistema* > *Restauração do Sistema*.

2 Insira o local do arquivo de backup. Pode ser um arquivo local, um arquivo de rede montado ou um arquivo em um dispositivo removível, como disquete ou DVD. Depois, clique em *Avançar*.

   A caixa de diálogo a seguir exibe um resumo das propriedades do arquivo, como nome de arquivo, data de criação, tipo de backup e comentários opcionais.

3 Revise o conteúdo do arquivo clicando em *Conteúdo do Arquivo*. Se você clicar em *OK*, retornará à caixa de diálogo *Propriedades do Arquivo*.

4 *Opções de Especialista* abre uma caixa de diálogo na qual é possível ajustar o processo de restauração. Retorne à caixa de diálogo *Propriedades do Arquivo* clicando em *OK*.

5 Clique em *Avançar* para abrir a exibição dos pacotes a serem restaurados. Pressione *Aceitar* para restaurar todos os arquivos do pacote, ou use os vários botões *Selecionar Tudo*, *Anular Seleção* e *Selecionar Arquivos* para fazer a sintonia fina da sua seleção. Somente use a opção *Restaurar Banco de Dados RPM* se o banco de dados RPM estiver corrompido ou tiver sido apagado e se esse arquivo estiver incluído no backup.

6 Depois que você clicar em *Aceitar*, o backup será restaurado. Clique em *Concluir* para sair do módulo após a conclusão do processo de restauração.

31.6.4 Recuperando um sistema corrompido

Há vários motivos pelos quais um sistema pode não ser inicializado ou executado adequadamente. Um sistema de arquivos corrompido após uma falha do sistema, arquivos de configuração corrompidos ou uma configuração de carregador de boot corrompida são os mais comuns.

O SUSE Linux Enterprise Desktop oferece dois métodos diferentes para resolver essas situações. Você pode usar a função YaST Reparo do Sistema ou inicializar o sistema de resgate. As seções a seguir abordam os dois tipos de métodos de conserto do sistema.

31.6.4.1 Usando o Reparo do Sistema do YaST

> **NOTA: Configurações de teclado e idioma**
>
> Se você mudar as configurações de idioma depois de inicializar, o teclado também será adaptado.

Antes de iniciar o módulo Reparo do Sistema do YaST, determine em que modo ele será executado para melhor atender às suas necessidades. Dependendo da gravidade e da causa da falha do sistema (bem como da sua experiência), existem três modos diferentes a escolher:

Reparo Automático
: Se o sistema falhou devido a uma causa desconhecida e você basicamente não sabe que parte do sistema é responsável pela falha, use *Reparo Automático*. Uma ampla verificação automatizada será executada em todos os componentes do sistema instalado. Para obter uma descrição detalhada deste procedimento, consulte “Reparo Automático” (p 471).

Reparo Personalizado
: Se o sistema falhou e você sabe qual é o componente responsável, poderá reduzir a extensa verificação do sistema com *Reparo Automático*, e limitar o escopo da análise do sistema a esses componentes. Por exemplo, se as mensagens do sistema antes da falha sugerirem a existência de um erro no banco de dados de pacotes, você poderá limitar o procedimento de análise e reparo para que apenas verifique e restaure esse aspecto do sistema. Para obter uma descrição detalhada deste procedimento, consulte “Reparo Personalizado” (p 473).

Ferramentas Especialista
: Se você já tem uma ideia clara do componente que falhou e como isso deve ser corrigido, pode ignorar as execuções de análise e aplicar diretamente as ferramentas necessárias para o reparo do componente relevante. Para obter informações detalhadas, consulte “Ferramentas Especialista” (p 474).

Escolha um dos modos de reparo descritos acima e prossiga com o reparo do sistema conforme explicado nas seções a seguir:

Reparo Automático

Para iniciar o modo de reparo automático do YaST Reparo do Sistema, proceda da seguinte maneira:

1 Insira o meio de instalação do SUSE Linux Enterprise Desktop na unidade de DVD.

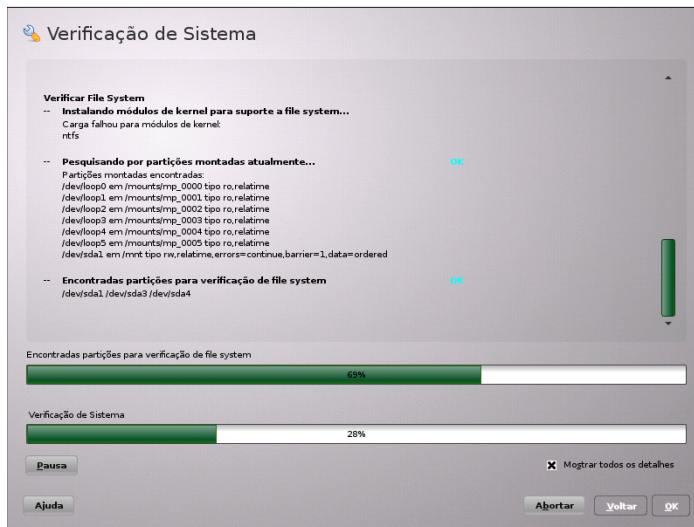
2 Reinicialize o sistema.

3 Na tela de boot, selecione *Reparar o Sistema Instalado*.

4 Confirme o contrato de licença e clique em *Avançar*.

5 Selecione *Reparo Automático*.

O YaST inicia uma ampla análise do sistema instalado. O progresso do procedimento é exibido na parte inferior da tela com duas barras. A barra superior mostra o progresso do teste atualmente em execução. A barra inferior mostra o progresso geral da análise. A janela de registro na seção superior controla o teste atualmente em execução e o seu resultado. Consulte a Figura 31.4, “Modo de Reparo Automático” (p 471).

Figura 31.4 *Modo de Reparo Automático*

As execuções de testes principais a seguir são feitas com cada execução e contêm, por sua vez, vários subtestes individuais:

Verificar Tabela de Partições
: Verifica a validade e coerência das tabelas de partição de todos os discos rígidos detectados.

Verificar Área de Swap
: As partições de troca do sistema instalado são detectadas, testadas e oferecidas para ativação, onde aplicável. Essa oferta deve ser aceita para que a velocidade de reparo do sistema aumente.

Verificar File System
: Todos os sistemas de arquivos detectados estão sujeitos a uma verificação específica de sistema de arquivos.

Verificar Entradas fstab
: As entradas no arquivo são verificadas quanto à totalidade e consistência. Todas as partições válidas são montadas.

Verificar Banco de Dados de Pacotes
: Verifica se todos os pacotes necessários para a operação de uma instalação mínima estão presentes. Embora seja opcionalmente possível analisar também os pacotes básicos, isso leva muito tempo, devido a seu grande número.

Verificar Configuração do Bootloader
: A configuração do carregador de boot do sistema instalado (GRUB ou LILO) é verificada quanto à totalidade e coerência. Dispositivos de boot e root são examinados e a disponibilidade dos módulos initrd é verificada.

6. Sempre que um erro é encontrado, o procedimento pára e uma caixa de diálogo com os detalhes e possíveis soluções é aberta.

   Leia as mensagens da tela com cuidado antes de aceitar a correção proposta. Se você decidir recusar uma solução proposta, seu sistema permanecerá inalterado.

7. Depois que o processo de reparo tiver terminado com sucesso, clique em *OK* e *Concluir* e remova a mídia de instalação. O sistema é reinicializado automaticamente.

Reparo Personalizado

Para iniciar o modo *Reparo Personalizado* e verificar seletivamente certos componentes do sistema instalado, proceda da seguinte maneira:

1 Insira o meio de instalação do SUSE Linux Enterprise Desktop na unidade de DVD.

2 Reinicialize o sistema.

3 Na tela de boot, selecione *Reparar o Sistema Instalado*.

4 Confirme o contrato de licença e clique em *Avançar*.

5 Selecione *Reparo Personalizado*.

A escolha de *Reparo Personalizado* mostra uma lista de execuções de testes que são todas marcadas inicialmente para execução. A faixa total de testes corresponde à faixa de reparo automático. Se você já sabe onde não há danos, desmarque os testes correspondentes. Clique em *Próximo* para iniciar um procedimento de teste mais restrito, que provavelmente tem um tempo de execução bem menor.

Nem todos os grupos de testes podem ser aplicados individualmente. A análise das entradas fstab está sempre atrelada a uma verificação dos sistemas de arquivo, incluindo partições de troca existentes. O YaST resolve automaticamente essas dependências selecionando o menor número de execuções de testes necessárias. O YaST não suporta partições criptografadas. Caso tenha uma, o YaST lhe informará sobre ela.

6 Sempre que um erro é encontrado, o procedimento pára e uma caixa de diálogo com os detalhes e possíveis soluções é aberta.

Leia as mensagens da tela com cuidado antes de aceitar a correção proposta. Se você decidir recusar uma solução proposta, seu sistema permanecerá inalterado.

7 Depois que o processo de reparo tiver terminado com sucesso, clique em *OK* e *Concluir* e remova a mídia de instalação. O sistema é reinicializado automaticamente.

Ferramentas Especialista

Se você tem experiência com o SUSE Linux Enterprise Desktop e já tem uma ideia muito clara do que precisa ser reparado no sistema, aplique as ferramentas diretamente e ignore a análise do sistema.

Para aproveitar o recurso *Ferramentas Especialistas* do módulo Reparo do Sistema do YaST, proceda da seguinte maneira:

1 Insira o meio de instalação do SUSE Linux Enterprise Desktop na unidade de DVD.

2 Reinicialize o sistema.

3 Na tela de boot, selecione *Reparar o Sistema Instalado*.

4 Confirme o contrato de licença e clique em *Avançar*.

5 Selecione *Ferramentas Especialista* e escolha uma opção de reparo.

6 Depois que o processo de reparo tiver terminado com sucesso, clique em *OK* e *Concluir* e remova a mídia de instalação. O sistema é reinicializado automaticamente.

As *Ferramentas Especialista* oferecem as seguintes opções para reparar a falha do sistema:

Instalar Novo Bootloader
: Isso inicia o módulo de configuração do bootloader do YaST. Encontre detalhes na Seção 12.2, “Configurando o carregador de boot com o YaST” (p 155).

Inicializar Sistema Instalado
: Tente inicializar um sistema Linux já instalado.

Iniciar Ferramenta de Particionamento
: Essa opção inicia a ferramenta de particionamento avançada no YaST.

Reparar Sistema de Arquivos
: Essa opção verifica os sistemas de arquivos do sistema instalado. Na seleção de todas as partições detectadas apresentada primeiro, escolha aquelas que deseja verificar.

Recuperar Partições Perdidas

É possível tentar reconstruir tabelas de partição danificadas. Uma lista de discos rígidos detectados é apresentada primeiro para seleção. Clicar em *OK* inicia a verificação. Isso pode demorar um pouco, dependendo da velocidade do seu computador e do tamanho e da velocidade do disco rígido.

IMPORTANTE: *Reconstruindo uma tabela de partição*

A reconstrução de uma tabela de partição é complicada. O YaST tenta reconhecer partições perdidas analisando os setores de dados do disco rígido. As partições perdidas são adicionadas à tabela de partição de reconstrução quando reconhecidas. Isso, no entanto, não é bem-sucedido em todos os casos imagináveis.

Gravar Configurações do Sistema em Disquete

Essa opção grava arquivos de sistemas importantes em um disquete. Se um desses arquivos ficar danificado, ele poderá ser restaurado a partir do disco.

Verificar Software Instalado

Isso verifica a consistência do banco de dados de pacotes e a disponibilidade dos pacotes mais importantes. Quaisquer pacotes instalados podem ser reinstalados com essa ferramenta.

31.6.4.2 Usando o sistema de recuperação

O SUSE Linux Enterprise Desktop inclui um sistema de recuperação. que consiste em um pequeno sistema Linux que pode ser carregado em um disco de RAM e montado como um sistema de arquivos raiz, permitindo acesso externo às partições Linux. Com o sistema de recuperação, você pode recuperar ou modificar qualquer aspecto importante do sistema:

- Manipule qualquer tipo de arquivo de configuração.
- Verifique se há defeitos no sistema de arquivos e inicie processos de reparo automáticos.
- Acesse o sistema instalado em um ambiente de “mudança de raiz”.
- Verifique, modifique e reinstale a configuração do carregador de boot.

- Recuperar-se de um driver de dispositivo instalado incorretamente ou um kernel inutilizável.

- Redimensione as partições usando o comando parted. Encontre mais informações sobre essa ferramenta no site GNU Parted na Web `http://www.gnu.org/software/parted/parted.html`.

É possível carregar o sistema de recuperação a partir de várias origens e locais. A opção mais simples é inicializar o sistema de recuperação a partir do meio original de instalação:

1. Insira o meio de instalação na unidade de DVD.

2. Reinicialize o sistema.

3. Na tela de boot, pressione F4 e escolha *DVD-ROM*. Em seguida, escolha *Sistema de Recuperação* no menu principal.

4. Digite `root` no prompt `Rescue:`. Não é necessário inserir uma senha.

Se a sua configuração de hardware não inclui uma unidade de DVD, você poderá inicializar o sistema de recuperação a partir de uma fonte na rede. O seguinte exemplo aplica-se a um cenário de boot remoto. Se você estiver usando outro meio de boot, como um DVD, modifique o arquivo `info` adequadamente e inicialize como em uma instalação normal.

1. Digite a configuração do seu boot PXE e adicione as linhas `install=`*`protocolo`*`://`*`fonte_de_instalação`* e `rescue=1`. Se precisar iniciar o sistema de recuperação, prefira `repair=1`. Como em uma instalação normal, *`protocolo`* significa qualquer um dos protocolos de rede suportados (NFS, HTTP, FTP, etc.) e *`origem_inst`* é o caminho da origem de instalação da rede.

2. Inicialize o sistema usando “Wake on LAN”, conforme descrito na Section “Wake on LAN” (Chapter 11, *Remote Installation*, ↑*Deployment Guide*).

3. Digite `root` no prompt `Rescue:`. Não é necessário inserir uma senha.

Depois de acessar o sistema de recuperação, você poderá utilizar os consoles virtuais por meio das teclas Alt + F1 a Alt + F6.

Um shell e muitos outros eficientes utilitários, como o programa de montagem, estão disponíveis no diretório /bin. O diretório sbin contém importantes utilitários de arquivo e de rede para a análise e o reparo do sistema de arquivos. Esse diretório também contém os binários mais importantes para a manutenção do sistema, por exemplo, fdisk, mkfs, mkswap, mount, mount, init e shutdown, assim como ifconfig, ip, route e netstat para a manutenção da rede. O diretório /usr/bin contém o editor vi, find, less e ssh.

Para ver as mensagens do sistema, use o comando dmesg ou exiba o arquivo /var/log/messages.

Verificando e manipulando arquivos de configuração

Como exemplo de uma configuração que possa ser corrigida por meio do sistema de recuperação, suponha que você tenha um arquivo de configuração defeituoso que impeça a inicialização adequada do sistema. Você pode corrigir isso usando o sistema de recuperação.

Para manipular um arquivo de configuração, faça o seguinte:

1. Inicie o sistema de recuperação usando um dos métodos descritos acima.

2. Para montar uma sistema de arquivos raiz localizado em /dev/sda6 para o sistema de recuperação, use o seguinte comando:

   ```
   mount /dev/sda6 /mnt
   ```

   Agora, todos os diretórios do sistema estão localizados em /mnt

3. Mude o diretório para o sistema de arquivos raiz montado:

   ```
   cd /mnt
   ```

4. Abra o arquivo de configuração problemático no editor vi. Ajuste e grave a configuração.

5. Desmonte o sistema de arquivos raiz no sistema de recuperação:

   ```
   umount /mnt
   ```

6. Reinicialize a máquina.

Reparando e verificando os sistemas de arquivos

Geralmente, não é possível reparar sistemas de arquivos em um sistema em execução. Se você tiver sérios problemas, talvez não consiga montar seu sistema de arquivos raiz e a inicialização do sistema poderá ser encerrada com “kernel panic”. Nesse caso, a única maneira será reparar o sistema externamente. É recomendável usar o YaST Reparo do Sistema para essa tarefa (consulte a Seção 31.6.4.1, “Usando o Reparo do Sistema do YaST” (p 470) para obter detalhes). Contudo, se você precisar fazer uma verificação ou um reparo manual no sistema de arquivos, inicialize o sistema de recuperação. Inclui os utilitários para verificar e consertar os sistemas de arquivos `btrfs`, `ext2`, `ext3`, `ext4`, `reiserfs`, `xfs`, `dosfs` e `vfat`.

Acessando o sistema instalado

Se você precisa acessar o sistema instalado do sistema de recuperação, faça isso em um ambiente *raiz de mudança*. Por exemplo, para modificar a configuração do carregador de boot ou executar um utilitário de configuração de hardware.

Para configurar um ambiente de mudança de raiz com base no sistema instalado, faça o seguinte:

1 Primeiro monte a partição raiz do sistema instalado e do sistema de arquivos do dispositivo (mude o nome do dispositivo de acordo com as suas configurações atuais):

```
mount /dev/sda6 /mnt
mount --bind /dev /mnt/dev
```

2 Agora, você pode “mudar a raiz” no novo ambiente:

```
chroot /mnt
```

3 Em seguida, monte `/proc` e `/sys`:

```
mount /proc
mount /sys
```

4 Por fim, monte as partições restantes no sistema instalado:

```
mount -a
```

5 Agora, você tem acesso ao sistema instalado. Antes de reinicializar o sistema, desmonte as partições com `umount -a` e saia do ambiente de “mudança de raiz” com `exit`.

ATENÇÃO: Limitações

Embora você tenha acesso total aos arquivos e aplicativos do sistema instalado, há algumas limitações. O kernel em execução é o que foi inicializado com o sistema de recuperação, e não com o ambiente de mudança de raiz. Ele suporta apenas o hardware essencial e não é possível adicionar módulos do kernel do sistema instalado, a menos que as versões do kernel sejam exatamente iguais. Verifique sempre a versão do kernel em execução (recuperação) com `uname -r` e, em seguida, descubra se existe um subdiretório correspondente no diretório `/lib/modules` no ambiente raiz de mudança. Em caso positivo, você poderá usar os módulos instalados; do contrário, precisará fornecer as versões corretas em outra mídia, como um pendrive USB. Na maioria das vezes, a versão do kernel de recuperação é diferente da que está instalada, portanto, não é possível simplesmente acessar a placa de som, por exemplo. Também não será possível iniciar uma interface gráfica de usuário.

Observe também que você sai do ambiente de “mudança de raiz” ao percorrer o console com as teclas Alt + F1 a Alt + F6.

Modificando e reinstalando o carregador de boot

Às vezes, não é possível reinicializar um sistema porque a configuração do carregador de boot está corrompida. As rotinas de inicialização não podem, por exemplo, converter unidades físicas em locais reais no sistema de arquivos Linux sem um carregador de boot ativo.

Para verificar a configuração do carregador de boot e reinstalá-lo, faça o seguinte:

1 Execute as etapas necessárias para acessar o sistema instalado como descrito em “Acessando o sistema instalado” (p 478).

2 Verifique se os arquivos a seguir estão configurados corretamente de acordo com os princípios de configuração do GRUB, descritos no Capítulo 12, *O carregador de boot GRUB* (p 143) e aplique as correções, se necessário.

- `/etc/grub.conf`

- `/boot/grub/device.map`
- `/boot/grub/menu.lst`
- `/etc/sysconfig/bootloader`

3 Reinstale o carregador de boot usando a seguinte sequência de comandos:

```
grub --batch < /etc/grub.conf
```

4 Desmonte as partições, efetue logout do ambiente de “mudança de raiz” e reinicialize o sistema:

```
umount -a
exit
reboot
```

Corrigindo a instalação do Kernel

Uma atualização do kernel pode introduzir um novo bug capaz de afetar a operação do sistema. Por exemplo, um driver de parte do hardware no sistema pode estar com falha, o que o impede de acessá-lo e usá-lo. Nesse caso, reverta para o último kernel em funcionamento (se disponível no sistema) ou instale o kernel original pela mídia de instalação.

DICA: Como manter os últimos kernels após a atualização

Para evitar falhas na inicialização após uma atualização do kernel com defeito, use o recurso multiversão do kernel e indique ao `libzypp` quais kernels deseja manter após a atualização.

Por exemplo, para sempre manter os dois últimos kernels e o kernel atual em execução, adicione

```
multiversion.kernels = latest,latest-1,running
```

ao arquivo `/etc/zypp/zypp.conf`.

Um caso semelhante é quando você precisa reinstalar ou atualizar um driver com defeito em um dispositivo não suportado pelo SUSE Linux Enterprise Desktop. Por exemplo, quando o fornecedor do hardware utiliza determinando dispositivo, como um controlador

RAID de hardware, que precisa de um driver binário para ser reconhecido pelo sistema operacional. O fornecedor, normalmente, lança um Disco de Atualização de Driver com a versão corrigida ou atualizada do driver necessário.

Nos dois casos, você precisa acessar o sistema instalado no modo de recuperação e corrigir o problema relacionado ao kernel; do contrário, o sistema poderá não ser inicializado corretamente:

1 Inicialize da mídia de instalação do SUSE Linux Enterprise Desktop.

2 Se você estiver recuperando após uma atualização do kernel com defeito, ignore esta etapa. Se precisar usar um disco de atualização de driver (DUD), pressione F6 para carregar a atualização de driver depois que o menu de boot aparecer e, em seguida, escolha o caminho ou URL para a atualização de driver e confirme clicando em *Sim*.

3 Escolha *Sistema de Recuperação* no menu de boot e pressione Enter. Se você usar o DUD, será solicitado a especificar o local em que a atualização de driver está armazenada.

4 Digite `root` no prompt `Rescue:`. Não é necessário inserir uma senha.

5 Monte manualmente o sistema de destino e "mude a raiz" para o novo ambiente. Para obter mais informações, consulte "Acessando o sistema instalado" (p 478).

6 Se você usar o DUD, instale/reinstale/atualize o pacote de driver do dispositivo com defeito. Sempre verifique se a versão do kernel instalada corresponde exatamente à versão do driver que está instalando.

Se você estiver corrigindo uma instalação de atualização do kernel com defeito, poderá instalar o kernel original da mídia de instalação com o procedimento a seguir.

6a Identifique o seu dispositivo de DVD com `hwinfo --cdrom` e monte-o com `mount /dev/sr0 /mnt`.

6b Navegue até o diretório em que os arquivos do kernel estão armazenados no DVD, por exemplo, `cd /mnt/suse/x86_64/`.

6c Instale os pacotes necessários `kernel-*`, `kernel-*-base` e `kernel-*-extra` de acordo com o seu tipo, usando o comando `rpm -i`.

6d Após o término da instalação, verifique se uma nova entrada de menu relevante ao kernel recém-instalado foi adicionada ao arquivo de configuração do carregador de boot (`/boot/grub/menu.lst` para `grub`).

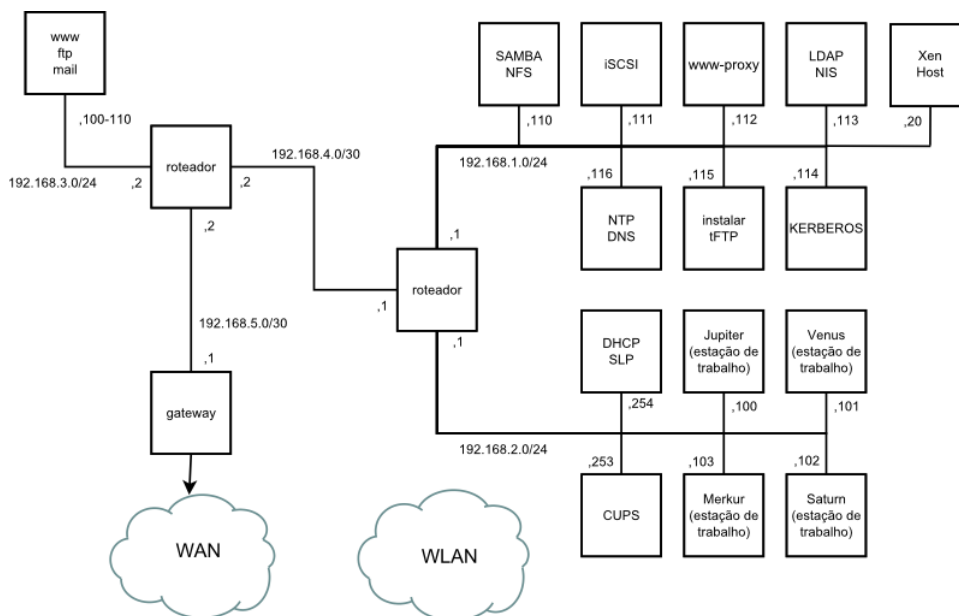
7 Atualize os arquivos de configuração e reinicialize o carregador de boot, se necessário. Para obter mais informações, consulte a “Modificando e reinstalando o carregador de boot” (p 479).

8 Remova a mídia inicializável da unidade do sistema e reinicialize-o.

Rede de exemplo

Este exemplo de rede é usado em todos os capítulos relacionados à rede na documentação do SUSE® Linux Enterprise Desktop.

GNU Licenses

B

This appendix contains the GNU Free Documentation License version 1.2.

GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.